Attack on Blockchain – Video Lecture from Youtube

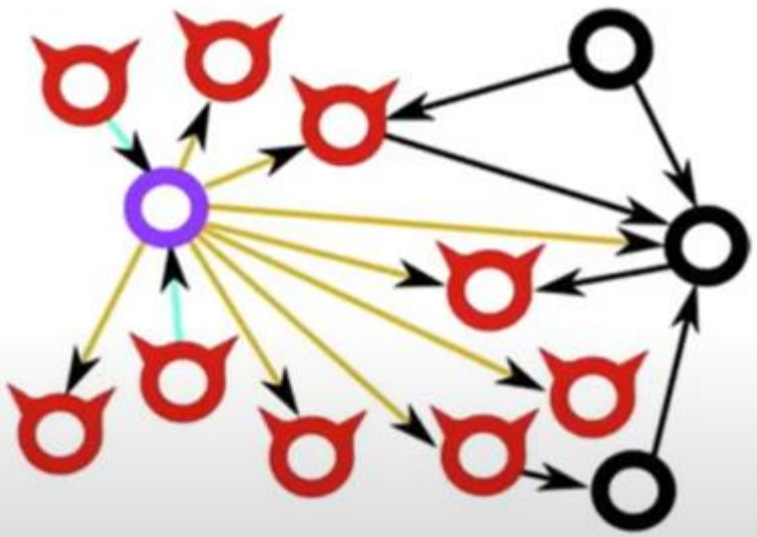
Categories

- Peer-to-peer network based attacks
  - Eclipse, Sybil
- Consensus Mechanism based attacks
  - Selfish mining, Mining malware, 51% attack, Timejack,Finney
- Smart contract based
  - The DAO attack
- Wallet based
  - Parity multisig wallet attack
- Traditional attacks on Blockchain services
  - Exchange hacks, DeFi Hack, Phishing, Rugpull/ExitScams, Ransomware, Fake software wallets

Peer-to-peer network based attacks

Eclipse Attack

- A node will depend on “x” number of nodes selected using a Peer selection strategy to have its view of the distributed ledger.
- But if an attacker can manage to make the node to choose all the “x” number of nodes from his malicious nodes alone, then he can eclipse the original ledger’s view and present his own manipulated ledger to the node.



Sybil Attack

- While the Eclipse attack is about eclipsing a user's view of the true ledger, the Sybil attack targets the whole network. In a Sybil attack, an attacker will flood the network with large number of nodes with pseudonymous identity and try to influence the network.
- These nodes, though appearing like unrelated individuals, are operated by a single operator at the back. In this case the objective is not to target one user, but a number of nodes or network as whole, and generate a fork in the ledger if possible, allowing the attacker to make double spending and other attacks.

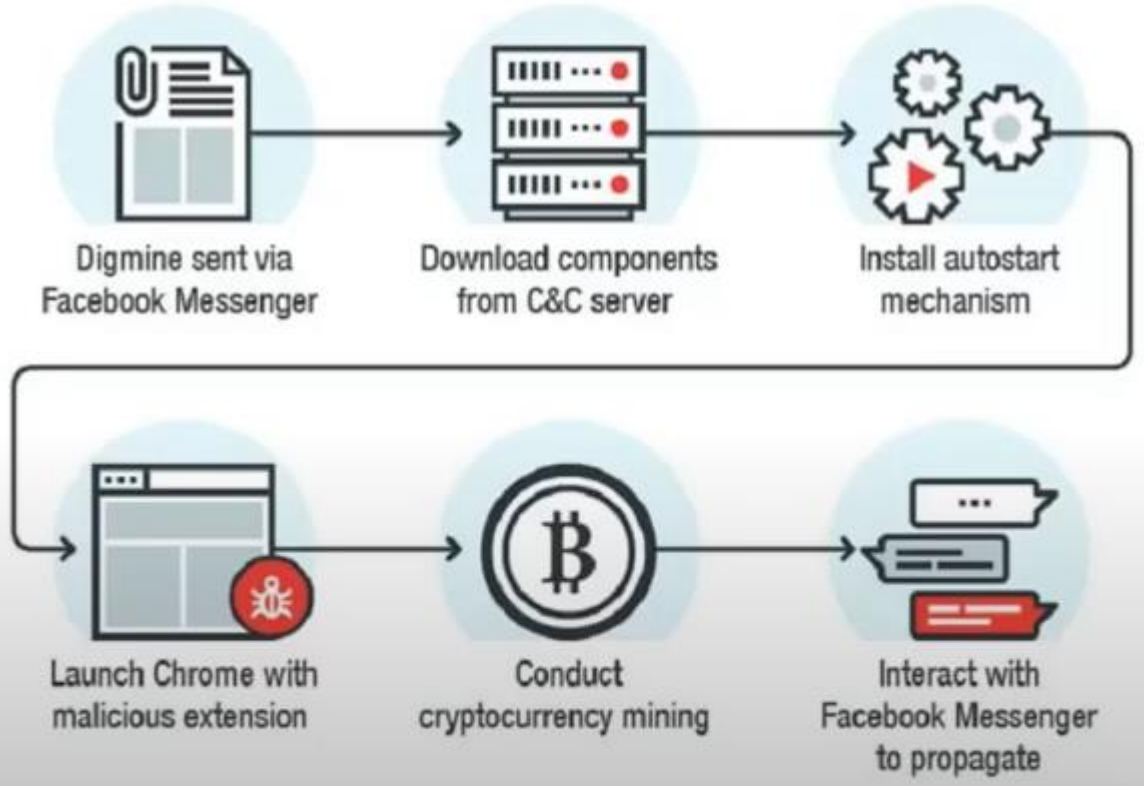
Consensus Mechanism based attacks

Selfish mining

- Many blockchains consider the longest chain to be the true latest version of the ledger. So a selfish miner can try to keep building blocks in stealth mode on top of the existing chain, and when he can build a lead of greater than two or more blocks than the current chain in the network, he can publish his private fork, which will be accepted as a new truth as it is the longest chain.
- He can do transactions in the public network just before publishing his longer stealth chain to reverse the transaction he just did. This effectively provides a small window for the attacker to do double spending based on this ability to build a stealth chain by building sufficient block lead (Finney attack)

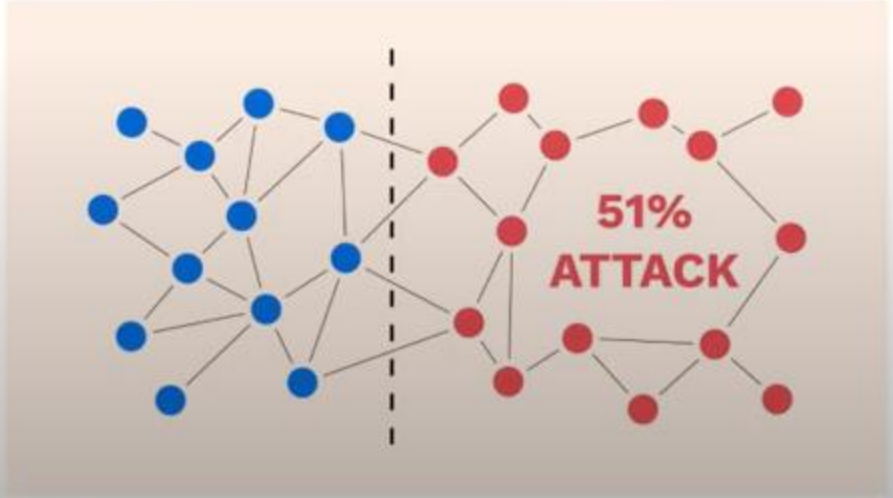
Mining malware

- Malware uses the computing power of unsuspecting victims' computer to mine cryptocurrencies for hackers. China reported that over a million computers were infected by this malware and helped attackers mine more than 26 million tokens of various cryptocurrencies.



51% attack

- This attack is possible when a miner or a group of miners controls 51% or more of the mining power of the blockchain network. Though it is very difficult to happen for large networks, the possibility of a 51% attack is higher in small networks. Once a group has majority control over transactions on a blockchain network, it can prevent specific transaction or even reverse older transactions.



Timejack Attack

- Nodes in certain blockchain networks like Bitcoin depend on internal timing derived from median time reported by its peer nodes. For example, you depend on your friends to know the time.
- Let us say an attacker manages to put a lot of malicious people in your friends' list, then he can manipulate your time. The first step to this attack can be an Eclipse attack on the target node. Once this attack is complete on a target node, then the target node will not accept blocks from the actual network as the timestamp of the blocks will not be in line with its timestamp.
- This provides an opportunity for the attacker to be double spending or do transactions with the targeted node as these transactions can't be submitted to the actual blockchain network.

Finney

- If you can mine a block with one of your transactions in it and keep it in stealth, there is an opportunity for you to double spend the money. If a merchant accepts the unconfirmed transaction, you can transfer him this earlier transacted currency.
- Next you publish the earlier mined block, which was kept in stealth, before your new transaction is confirmed on network

Smart Contract-based Attacks

The DAO attack

- The biggest exploitation in the history of cryptocurrencies is the “THE DAO” hack. Decentralized Autonomous Organization was an ambitious feature of Ethereum. A company called Slock started crowdfunding for a project called “The DAO”. The crowdfunding got an overwhelming response, collecting 12.7 million Ether, valued at $150 million then ($2 billion today).
- But an attacker identified a vulnerability in the code where by a recursive withdraw function could be executed without checking the settlement of the current transaction. So the attacker started the attack by contributing a small amount and requesting withdrawal with a recursive function. This allowed him to pull out almost $70 million dollars out of the crowdfund.

Traditional attacks on Blockchain services

Exchange hacks

- The Exchanges built around cryptocurrencies are central in nature, attracting hackers. As these exchanges are central in nature they are vulnerable to various traditional hacking techniques.
- Once an exchange is hacked the user data can be used to extract all or majority of the funds in the hackers account.

DeFi Hack

- It's common for attackers to fund DeFi attacks through flash loans, which require no collateral or Know-Your-Customer (KYC) identification data, making it increasingly difficult to catch bad actors.
- The attacker used flash loan ETH from a decentralized cryptocurrency exchange to repeatedly fund deposits into the liquidity pool—thereby artificially inflating the value—and withdraw more ETH than initially deposited due to the inflation.

Phishing

- Phishing attacks are all too common in and outside of the blockchain economy.
- Increasingly common in the crypto-space are very targeted spear-phishing attacks. In these types of attacks, the criminal has additional details on a victim that they can use to customize their attacks and often appear to come from much more trusted sources.

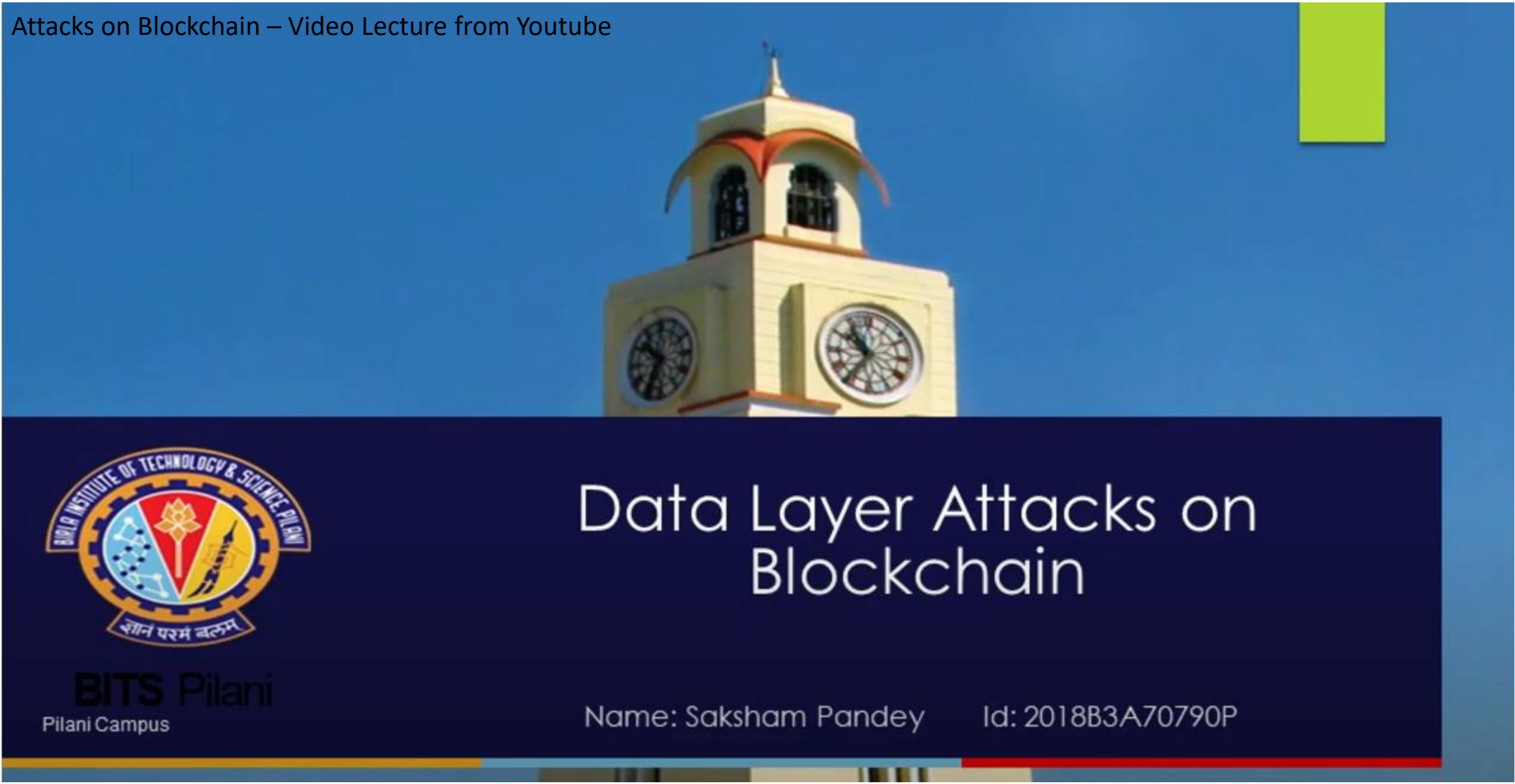
Rugpull / Exitscams

- In the crypto-verse, an exit scam refers to when an exchange disappears with user funds, seemingly out of the blue, leaving customers unable to withdraw from their accounts. This is typically the result of one or more members of the executive team misappropriating user funds and can be either planned from the inception of the exchange or happen suddenly due to inadequate safeguards to prevent embezzlement.

Fake software wallets

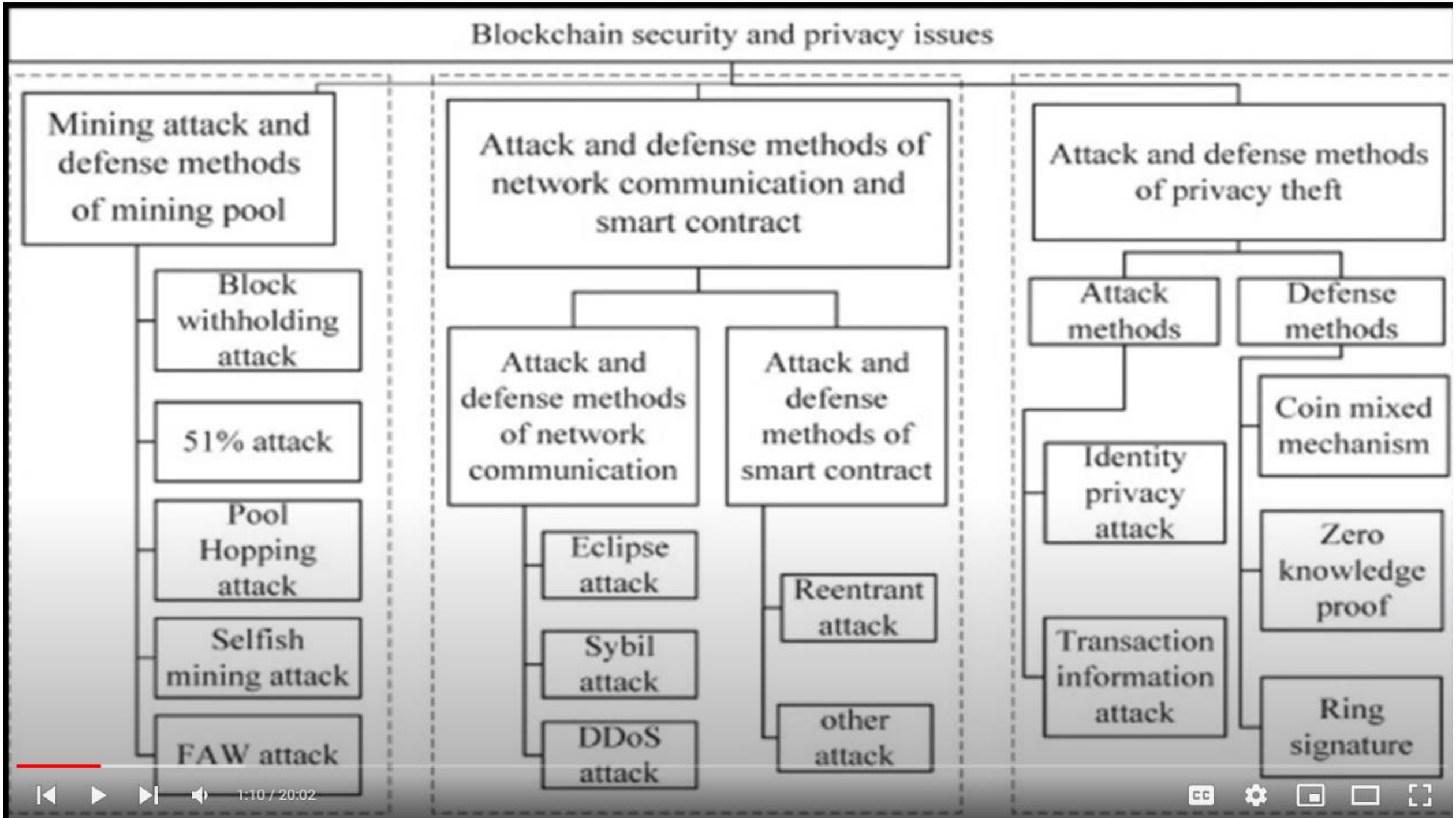
- Creating a mobile application and getting it into the Apple or Google Play app stores requires work, but it is of course not impossible.
- Creating a fake wallet app and trapping users can result in complete emptying of the user's crypto wallet.

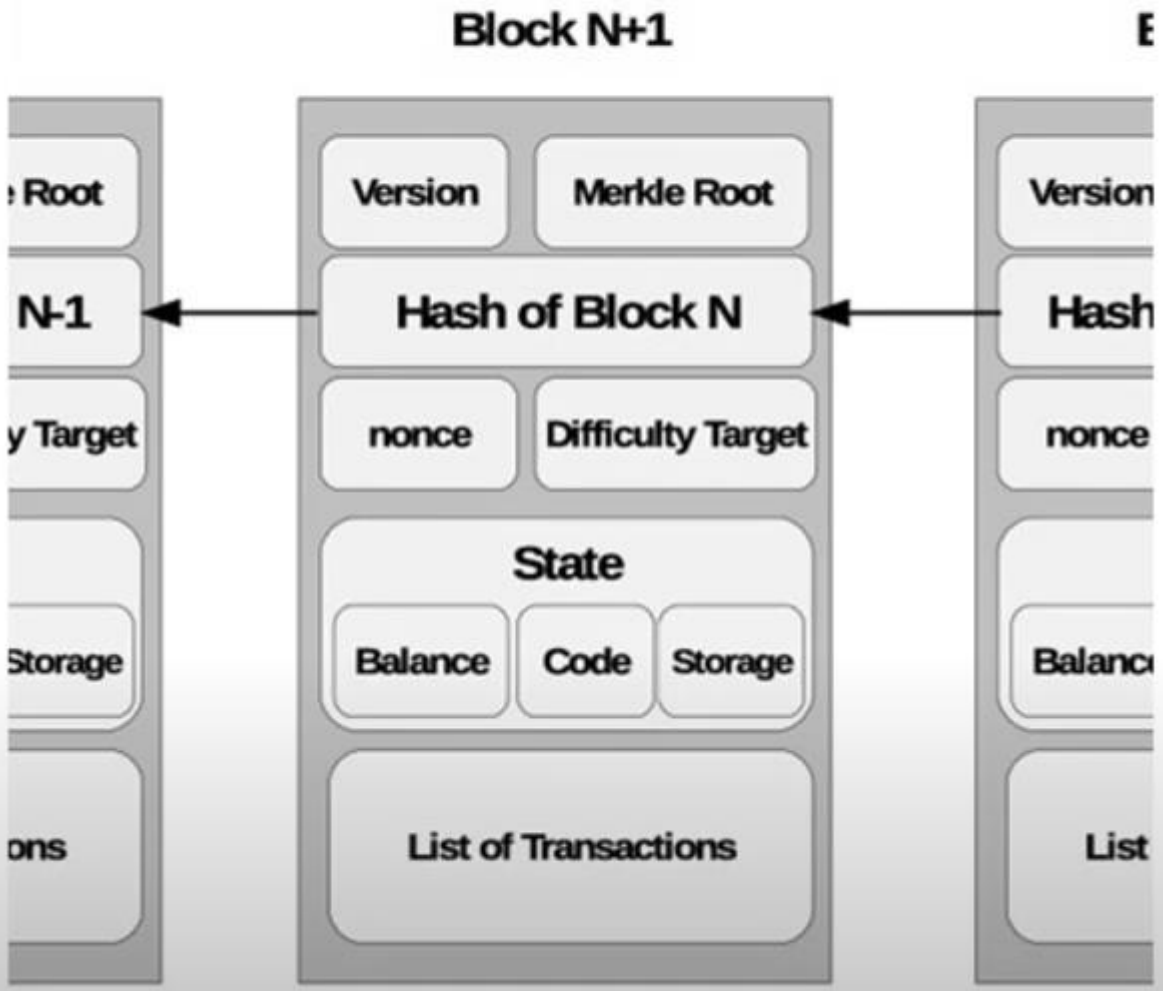
Attacks on Blockchain – Video Lecture from Youtube



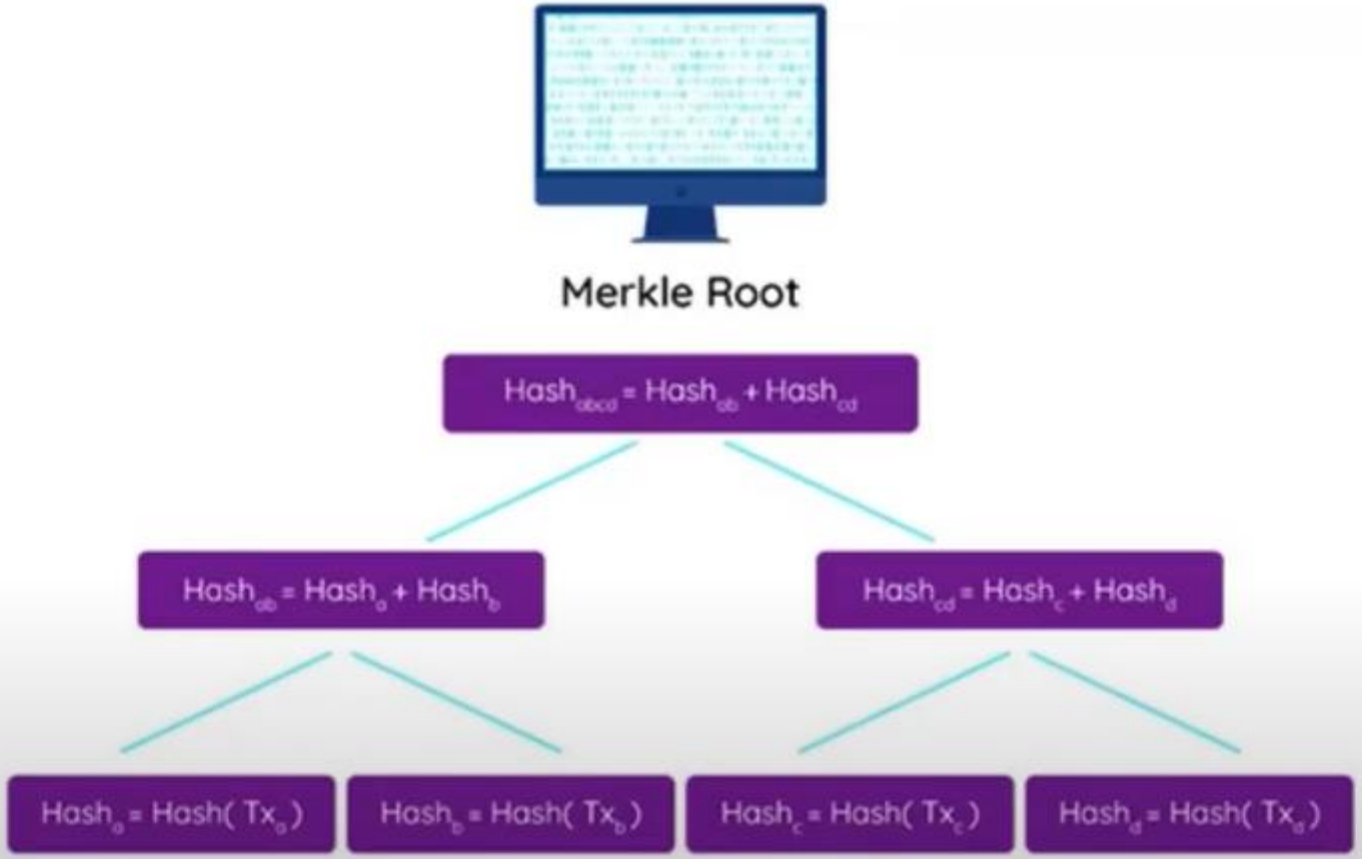
Outline

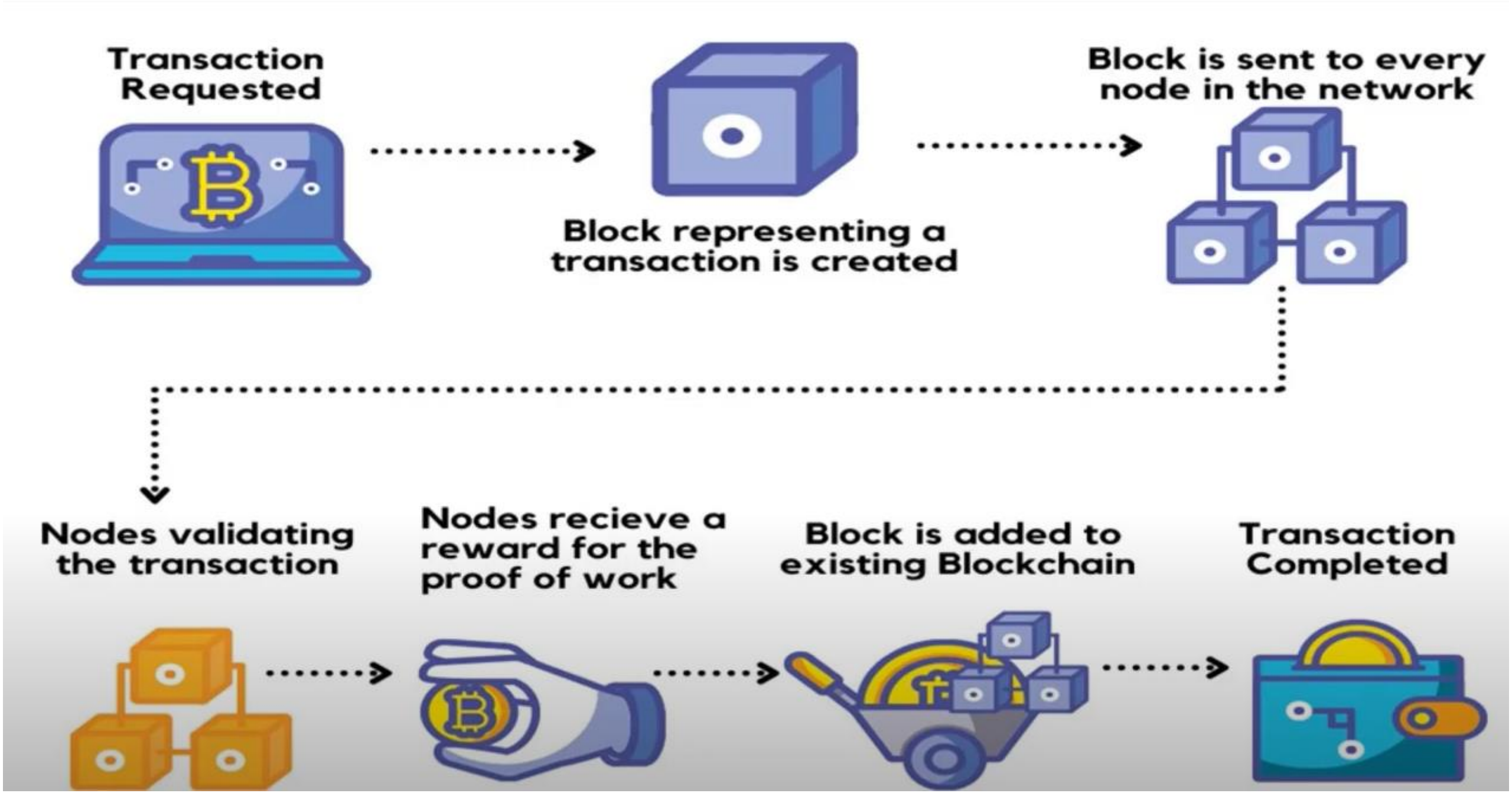
Introduction about attacks
What is a Data Layer?
Attacks on Data Layer
Defense Methods

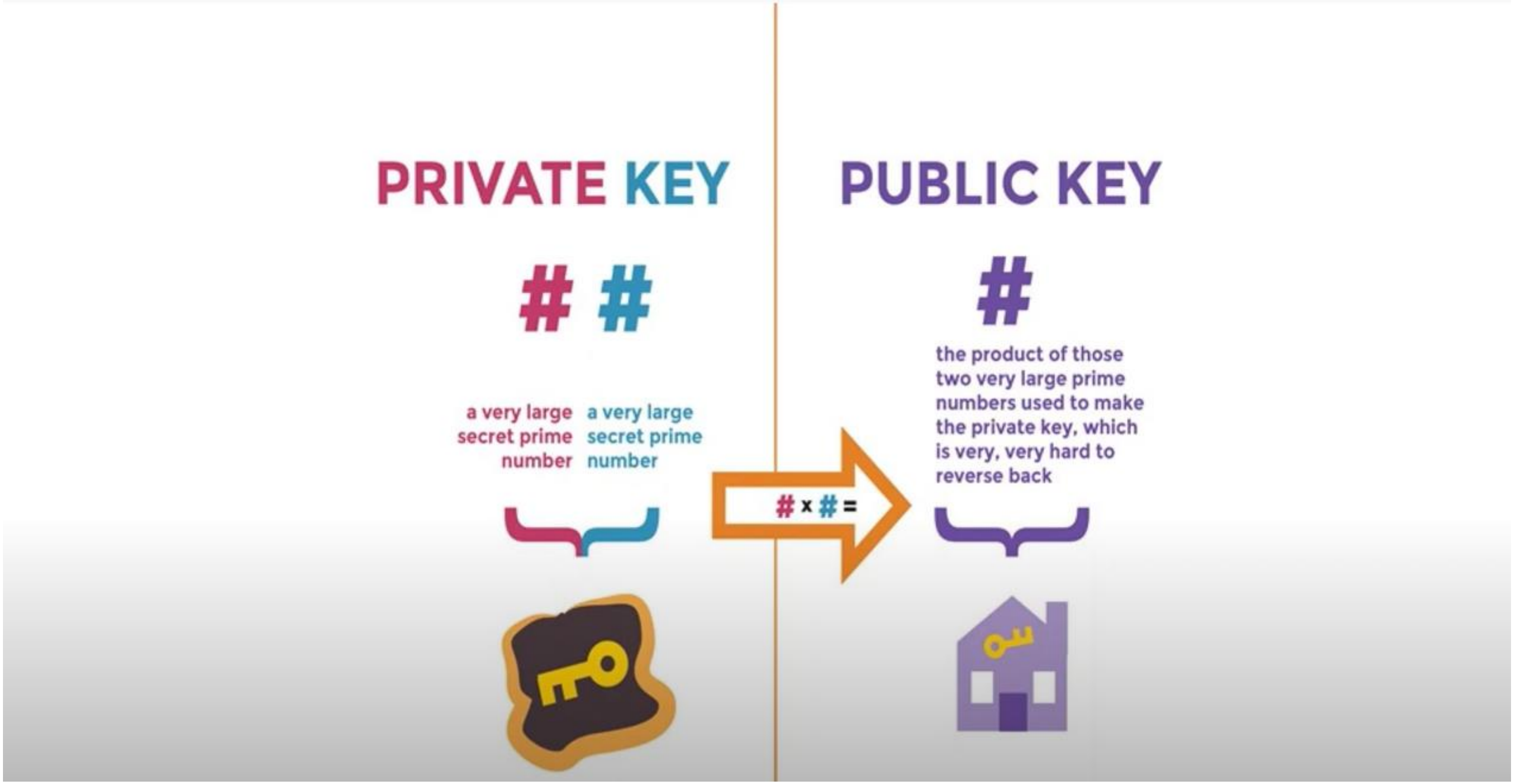

Blockchain security and privacy issues
Mining attack and defense methods of mining pool
Block withholding attack
51% attack
Pool Hopping attack
Selfish mining attack
FAW attack
Attack and defense methods of network communication and smart contract
Attack and defense methods of network communication
Eclipse attack
Sybil attack
DDoS attack
Attack and defense methods of smart contract
Reentrant attack
other attack
Attack and defense methods of privacy theft
Attack methods
Defense methods
Identity privacy attack
Transaction information attack
Coin mixed mechanism
Zero knowledge proof
Ring signature
1:10 / 20:02



Metadata of Block


Merkle Root
$Hash_{abcd} = Hash_{ab} + Hash_{cd}$
$Hash_{ab} = Hash_a + Hash_b$
$Hash_{cd} = Hash_c + Hash_d$
$Hash_a = Hash(Tx_a)$
$Hash_b = Hash(Tx_b)$
$Hash_c = Hash(Tx_c)$
$Hash_d = Hash(Tx_d)$


Transaction Requested
Block representing a transaction is created
Block is sent to every node in the network
Nodes validating the transaction
Nodes recieve a reward for the proof of work
Block is added to existing Blockchain
Transaction Completed

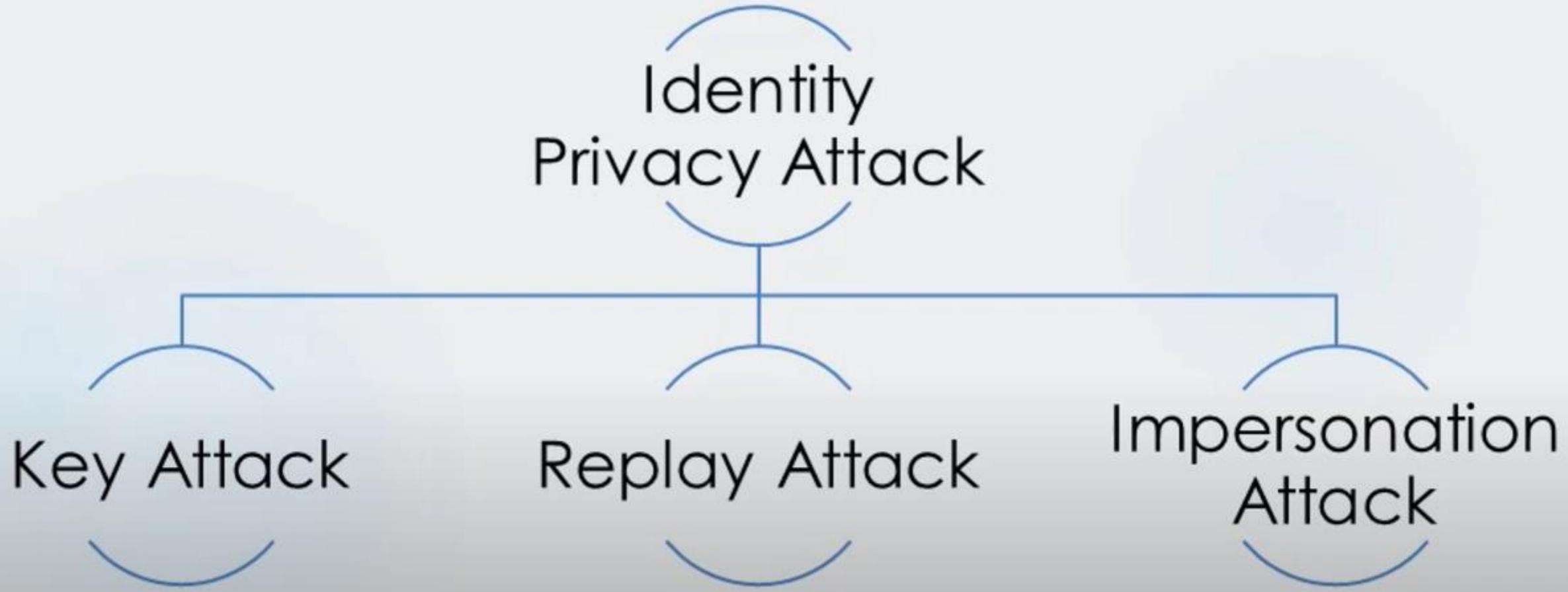

PRIVATE KEY
# #
a very large secret prime number
a very large secret prime number
x # =
PUBLIC KEY
#
the product of those two very large prime numbers used to make the private key, which is very, very hard to reverse back

Policy

Tether Froze $300K of Stablecoin Hacked After Victims Left Wallet Keys in Evernote

The U.S. government is pursuing a civil forfeiture claim on the more than 300,000 units of the tether (USDT) cryptocurrency said to have been stolen earlier this year.

By Sebastian Sinclair · Oct 26, 2020 at 2:35 p.m. Updated Sep 14, 2021 at 3:53 p.m.


Identity
Privacy Attack
Key Attack
Replay Attack
Impersonation
Attack

Transaction privacy Leakages

- User behaviours are traceable on blockchain networks.
- Transaction information attack means that the attacker uses the transaction diagram to analyse its potential information

Monero and Chaff coins

Monero transactions do not specify which previous outputs are being spent but list of fakes coins and one real one.

Transaction History

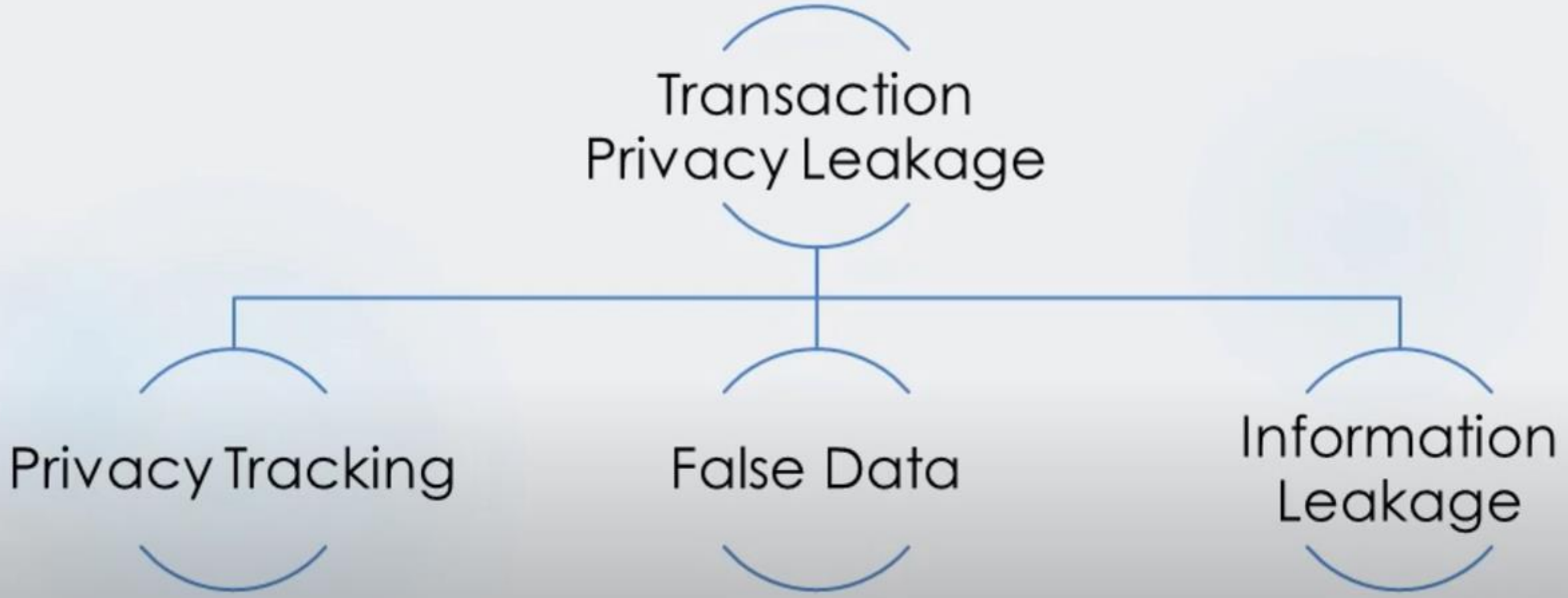
Print Export

10 Days

Smart Search: Account ID, Title, Transaction Type, Method

Date	Account ID	Title	Type	Method	Amount/Position	Status
2014-11-21	[illegible]	[illegible]	Deposit	CHECK	USD 234.00	Pending Receipt
2014-11-21	[illegible]	[illegible]	Deposit	CHECK	USD 40.00	Pending Receipt
2014-11-21	[illegible]	[illegible]	Deposit	WIRE	USD 23,021.00	Pending Receipt
2014-11-21	[illegible]	[illegible]	Deposit	WIRE	USD 98.00	Pending Receipt
2014-11-20	[illegible]	[illegible]	Withdrawal	WIRE	GBP 105.00	Cancelled
2014-11-20	[illegible]	[illegible]	Withdrawal	WIRE	USD 29.00	Pending
2014-11-18	[illegible]	[illegible]	Withdrawal	WIRE	USD 61.00	Not Confirmed
2014-11-17	[illegible]	[illegible]	Withdrawal	WIRE	USD 32.00	Not Confirmed
2014-11-17	[illegible]	[illegible]	Withdrawal	WIRE	USD 23.00	Not Confirmed
2014-11-17	[illegible]	[illegible]	Deposit	WIRE	GBP 2.00	Pending Receipt
2014-11-13	[illegible]	[illegible]	Withdrawal	WIRE	USD 11.00	Not Confirmed
2014-11-11	[illegible]	[illegible]	Withdrawal	WIRE	USD 1,000.00	Not Confirmed

The transaction information is disclosed anonymously, using this attack, the attacker can download all the transaction history of the Bitcoin and will use to analyze the user's associated transaction graph and behaviour of operation

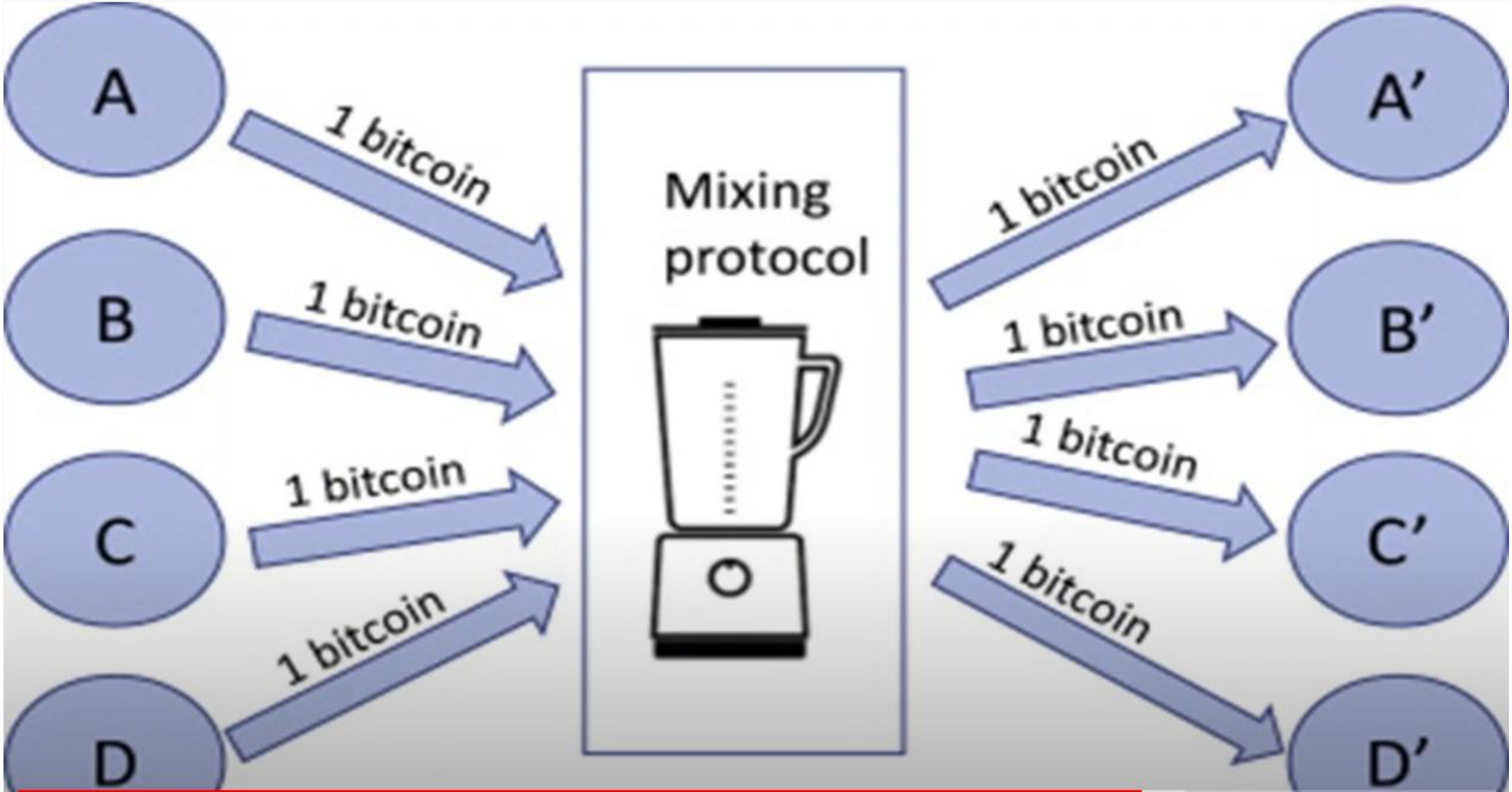

Transaction Privacy Leakage
Privacy Tracking
False Data
Information Leakage

Privacy Tracking

False Data

- Attackers can link different fragments of user using public key and deanonymize the user.
- This might give power to attacker to falsify and corrupt the information.

CONFIDENTIAL DATA


A
B
C
D
1 bitcoin
1 bitcoin
1 bitcoin
1 bitcoin
Mixing protocol
1 bitcoin
1 bitcoin
1 bitcoin
1 bitcoin
A'
B'
C'
D'

15:13 / 20:02

Dash Coin

- This digital currency uses the coin mixing mechanism.
- It comprises of two layers
  - First Layer: Miners use mining methods for network security protection.
  - Second Layer: Networks bundle transactions in a mix and send them when multiple funds are combined to achieve privacy protection.

Zero Knowledge Proofs

Zero Knowledge Proof

A digital currency Zerocoin by considering that the realization of the Mixcoin protocol requires the user's complete trust.

It breaks connection between the individuals in a transaction so as to prevent disclosing the information.

The combination of digital currency and zero-knowledge proof technology zk-SNARK enables the sender to prove their corresponding assets using mathematics.

Bitcoin – Video Lecture from Youtube

BITCOIN

WHAT IS BITCOIN?

Bitcoin is a digital currency.

It uses the peer-to-peer bitcoin network and doesn’t have any central bank or administrator.

Transactions are recorded in a ledger called a blockchain.

HISTORY

The domain name of bitcoin.org was registered in 2008. Later in the same year a link to paper authored by Satoshi Nakamoto was posted to a cryptography mailing list, titled “Bitcoin: A Peer-to-Peer Electronic Cash System”.

HISTORY

On January 3 2009, the bitcoin network came into existence with Satoshi Nakamoto mining the “genesis block of bitcoin”, which had a reward of 50 bitcoins.

On January 9 2009, the first open source bitcoin client was released, hosted at SourceForge.

HISTORY

The first retail transaction involving physical goods was paid on May 22, 2010, by exchanging 10000 BTC for two pizzas.

By 2011, other cryptocurrencies began to emerge, based on bitcoin's open-source code.

In 2012, the Bitcoin Foundation was founded.

Blockchain

A blockchain is a chain of blocks of information.

Every block contains a hash of the previous block upto the genesis block.

Any contract between two parties can be established on a blockchain if both parties agree, removing the need for a third party intermediary.

These blocks of transactions are distributed, which means anybody can access them.

Blockchain

At an an average of 10 minutes, a new block is added to the chain, and broadcasted across the network. This way double-spending can be prevented.

Transactions

When a user sends bitcoins, the user designates each address and the amount of bitcoin being sent to that address in an output. To prevent double spending, each input must refer to a previous unspent output in the blockchain. The user can add an optional transaction fee to incentivize miners to verify their transaction.

Mining

Since every node on the network maintains its own copy of ledger, the ledgers must be same across the network. The network trusts the ledger that has the most computational work put into it.

This ensures that a fraudulent transaction will require an infeasible amount of computation to be recorded into the ledger.

Mining

Miners add blocks to the chain. To add a block, they have to find a number, which when hashed (using SHA 256) with the block, gives a numerical value lesser than the networks difficulty target.

The difficulty target varies with an aim to keep average duration between block creation 10 minutes.

Wallet

A wallet stores the digital credentials for your bitcoin holdings like your public and private key for digital signing.

Decentralized Finance (DeFi) –Video Lecture from Youtube

What is DeFi

Decentralized Finance, or DeFi, refers to a set of applications built on top of blockchains that allow users to participate in financial transactions without needing a central authority or an intermediary.

DeFi applications give users more control over their assets and give users a more secure and transparent way of dealing with it.

Traditional Finance

Up until now, any means of exchanging assets among individuals has involved a third party. This third party can be a bank, an exchange, or even the government.

These third parties can charge you a fee, monitor your transactions or even block them for any reason they deem fit.

By participating in any financial exchange, we essentially have to trust these third parties to do their function well.

We give our money to banks because they promise to keep it safe and give you an "interest" on it. In doing so, we trust the bank to not make too many risky investments, ie, not give out bad loans.

When you want to transfer money to a friend, you have to go to your bank, initiate the transfer. Your friend will have to go to their bank and cash out the money they received. In this transaction, both banks can charge any fees they want.

Why DeFi Then?

DeFi eliminates the need for a third party.

Intermediaries like banks are replaced by literal pieces of code.

All transactions are verifiable by all the parties involved since they are stored on an immutable ledger.

There are smaller transaction fees because there's no for-profit party involved.

Since all transactions over the blockchain are pseudonymous, they cannot be regulated by the government for any reason.

The ERC20 Standard

To make the process of making tokens simpler, Ethereum introduced a standard called the ERC-20 standard.

ERC-20 establishes a set of “rules” for fungible tokens on the Ethereum chain. Every token compliant with the ERC-20 standard, has to expose a defined set of methods.

ERC-20 itself is a token that can be traded on top of the Ethereum chain.

The ERC-20 standard has enabled developers to build tokens that are interoperable with each other and simplified the API.

Today, most tokens built on the Ethereum chain are ERC-20 compliant.

```
function name() public view returns (string)
function symbol() public view returns (string)
function decimals() public view returns (uint8)
function totalSupply() public view returns (uint256)
function balanceOf(address _owner) public view returns (uint256 balance)
function transfer(address _to, uint256 _value) public returns (bool success)
function transferFrom(address _from, address _to, uint256 _value) public returns (bool success)
function approve(address _spender, uint256 _value) public returns (bool success)
function allowance(address _owner, address _spender) public view returns (uint256 remaining)
```

Applications of DeFi

Stable coins

Cryptocurrencies are widely considered to be volatile assets.

You wouldn't want to invest money in an asset that is so volatile.

Not all cryptocurrencies last in the market. Some of them are hypetrains while others are pump-and-dump schemes.

For any financial system to function well, it needs to be built upon a stable base. This is where stablecoins come in.

Stablecoins are "pegged" against a stable asset. This stable asset can be anything: a fiat currency, gold, silver, etc.

Stablecoins are a common way of holding your investments while mitigating the risk of volatility.

Stable Coins: Tether

Tether(USDt) is a stablecoin that is pegged to the US dollar. This means that 1 USDT ~= $1.

Tether allows you to trade more volatile coins in exchange for USDt coins that are much more stable. So, instead of selling your coins, you can simply trade them and avoid all of the fees and taxes.

Stablecoins like Tether also allow you to transfer funds around the globe for a very small fee.

In countries suffering from hyperinflation or excessive government intervention, stablecoins have become a way for people to save their money in a more secure asset than their fiat currency.

Since Tether is programmable, you can write smart contracts to transfer money to someone at a specific time, at specific intervals, or on the satisfaction of some condition. All without human intervention.

There are companies now which leverage this programmability to allow their employees to accept their salaries in crypto.

Tether : How?

We learned that 1 USDt is roughly equivalent to 1 USD. But how does that work?

When you buy Tether from a crypto exchange, the exchange transfers fiat currency into Tether's bank account.

In exchange, Tether issues an equivalent number of Tether tokens and transfers them to the user's wallet (minus the fees).

Now the user can do whatever they want with these tokens.

When the user decides to exchange these tokens for fiat currency, they can transfer these tokens back to Tether.

Tether will then remove these tokens from circulation and return the equivalent amount of currency from its bank account to the user's bank account.

This way, there's only as many Tether tokens in circulation as there are US dollars in Tether's bank account. Thus, one token will always be equal to one US dollar.

7:23 / 16:49

Lending & Borrowing

Now that we have a stable asset to deal in crypto, we can move on to more complex functions.

DeFi protocols enable users to lend and borrow assets among each other without the need for a third party. Essentially functioning like a decentralized bank.

Aave is one such protocol. Aave is built on top of the Ethereum chain.

Technically, Aave is a peer-to-smart-contract protocol.

Lenders can deposit money into a smart contract. Borrowers can deposit a collateral and in exchange borrow from any smart contract.

The name Aave comes from the Finnish word for “ghost”. The name also signifies that the protocol is completely anonymous.

Aave: Overcollateralization

Where there are loans, there has to be collateral involved. When taking a loan from a bank, you can place, lets say, your house as collateral.

This isn't how it works in crypto. When taking cryptocurrencies as a loan, you need to deposit some other crypto as collateral.

Aave loans are "overcollateralized". This means that you can only borrow X% of the money you placed as collateral.

Let's suppose this X is 80%. This means that you will have to place $100 of Ether to get $80 worth of USDt.

This sounds absurd at first. Why would you pay more collateral than you want to borrow? And if you already have more money than you need then why take a loan?

Aave: Overcollateralization

Let's continue with the last example. You put up $100 of Ethereum to borrow $80 of Tether.

You get to keep this and $80 and do what you please with it. Later, when Ethereum grows in price to lets say $200, you can give the $80 USDT back to get back $200.

These type of loans allow individuals to create leveraged positions and gain higher profits on a smaller amount of capital.

Loans in Aave also differ from traditional loans in the sense that there is no fixed time period to pay back the loan. However, as time grows your health score would decrease and make your investment more likely to get liquidated.

Aave has a certain liquidation threshold after which it automatically sells your collateral to the lenders. This way, lenders never lose money.

Decentralized Exchanges

Crypto being decentralized doesn't count for much if you're forced to trade it through a centralized exchange.

To deal with a centralized exchange, first you need to identify yourself via a KYC. They are for-profit entities and extract a fee for every transaction on their platform.

Instead of being governed by a central authority, decentralized exchanges, DEXes, work using smart contracts. They also have their governance tokens which are used to make decisions on the functioning of the DEX.

A DEX has a few limitations though. You can only use a DEX to swap tokens on the same blockchain.

Since there is no governing body, there is no support either. If you make a mistake (like transferring to a wrong address), there is no one to help you.

DEXes also suffer from low liquidity. This means that large orders can result in a significant amount of price fluctuation.

The Uniswap Protocol

Uniswap, built on top of the Ethereum blockchain, can be used to swap ERC-20 compatible tokens.

Since Uniswap is a decentralized exchange and there is no central body involved, the fees for a transaction are very low as compared to a centralized exchange.

Unlike a traditional market, Uniswap does not function on the order-book system.

Instead, Uniswap uses an automated market maker.

An automated market maker is a collection of smart contracts that define a standard way to create liquidity pools, provide liquidity, and swap assets.

Liquidity Pools

A liquidity pool is a pool containing two different assets.

In DeFi, a liquidity pool is nothing but a smart contract that can hold two different assets and transfer them. A liquidity pool lets you swap one asset with another for a very small transaction fee.

A liquidity pool always starts with a 50:50 ratio of both assets.

The more of one token is bought, the more its price increases.

For example, let's say you start a liquidity pool with ETH and BAT.

The more of BAT you buy in exchange for ETH, the more you'll be charged for a BAT.

This is done because the more of ETH you give to the liquidity pool, the more the algorithm thinks that it's price is dropping.

Liquidity pools also function as a means of investment. The people who provide the initial liquidity to the pool are known as liquidity providers.

These providers distribute the profits earned by the transaction fees.

Is DeFi actually the future?

Dangers Involved in DeFi

Since the technologies behind DeFi are still young, they are susceptible to attacks.

Most of the code involved in DeFi applications is open sourced. While this is a good thing as we can verify its behaviour ourselves, it also means that hackers have easier ways of finding out bugs in that code.

Cryptocurrencies have become a playground of choice for scammers. There's news of a new scam involving crypto almost everyday.

Since there is no regulation involved, the risks are higher. Traditional banks are governed by a clearly defined set of regulations. This is not true for DeFi applications. Hence, they don't offer the same amount of protection.

ERC Token – Video Lecture from Youtube

Ethereum Request for Comments(ERC)

ERC-20 Tokens

- ERC20 tokens exists on Ethereum platform and aren't independent and rely on Ethereum's blockchain and platform.
- The native currency on the Ethereum network is Ether. but besides Ether, it can also support other tokens.
- These tokens can work like (i) Currency
  (ii) shares of a company
  (iii) Gold certificates
  (iv) loyality points….

How are Ethereum Tokens Created

Smart Contracts(i) Creates Token
(ii) handles Transactions
(iii) Keeps Track balances

7 Ether

SMART CONTRACT

17 ERC-20 Tokens

SMART C

also Problem of Interoperability

- ERC20 is a guideline or standard for when you want to create your own token
- It has 6 mandatory Functions and 3 optional Functions that a Smart Contract should implement.

(i) TotalSupply
(ii) BalanceOf
(iii) Transfer
(iv) TransferFrom
(v) Approve
(vi) Allowance

- ERC-20 guideline and people are free to implement the required functions however they like. This lead to some Interesting Problems

18 ERC tokens sent
Instead of Ether

SMART CONTRACT

LOST!!!!!!

To Solve this ERC 223 token is Introduced

Token Tracker | Etherscan | MyEtherWallet | MEW | MyEtherWallet Simplex | Token Factory

myetherwallet.com

ETH | Swap | DApps | Tokens

MEW supports ETH and all ERC-20 tokens!

Tether (USDT)	Uniswap (UNI)	Chainlink (LINK)
USD Coin (USDC)	Wrapped Bitcoin (WBTC)	Crypto.com Coin (CRO)
Aave (AAVE)	OKB (OKB)	Binance USD (BUSD)
FTX Token (FTT)	cUSDC (CUSDC)	Dai (DAI)
Chiliz (CHZ)	cETH (CETH)	cDAI (CDAI)

Get tokens

More

Hide

SKALE

Get the official MEW wallet app

Download on the App Store

GET IT ON Google Play

SKL Staking new on iOS!

9:38 / 22:39

Token Tracker | Etherscan | MyEtherWallet | MEW | MyEtherWallet Simplex | Token Factory

etherscan.io/tokens

Etherscan

All Filters | Search by Address / Txn Hash / Block / Token / Ens

Eth: $2,641.03 (-3.99%) | 65 Gwei

Home | Blockchain | Tokens | Resources | More | Sign In

Token Tracker ERC-20

ERC-20 Tokens

A total of 495,485 Token Contracts found

First | Page 1 of 19 | Last

#	Token	Price	Change (%)	Volume (24H)	Circulating Market Cap	On-Chain Market Cap	Holders
1	Tether USD (USDT) Tether gives you the joint benefits of open blockchain technology and traditional currency by converting your cash into a stable digital currency equivalent.	$1.001 0.000026 Btc 0.000379 Eth	0.05%	$32,958,333,201.00	$79,147,776,327.00	$39,862,942,964.85	4,449,021 0.028%
2	BNB (BNB) Binance aims to build a world-class crypto exchange, powering the future of crypto finance.	$442.8586 0.011557 Btc 0.167684 Eth	1.87%	$3,362,542,087.00	$73,869,318,260.00	$7,342,381,227.88	321,491 0.003%
3	USD Coin (USDC) USDC is a fully	$1.00 0.000026 Btc	-0.09%	$2,170,683,871.00	$52,686,616,494.00	$46,602,430,840.00	1,374,[illegible] 0.041%

10:56 / 22:39

Token Tracker | Etherscan | Token Factory

Not secure | thetokenfactory.com/#/factory

Block Number: 0. 0s. Home Interact With Token Contract Create Token Contract YOU ARE OFFLINE.

Create Token

Create Token Contract with the following parameters.

totaly supply: eg. 10

name: eg Simon Bucks

decimal places: eg 4

symbol: eg SBX

Create Token

11:41 / 22:39

Token Tracker | Etherscan

Token Factory

Not secure | thetokenfactory.com/#/factory

Block Number: 0. 0s. Home Interact With Token Contract Create Token Contract YOU ARE OFFLINE.

Create Token

Create Token Contract with the following parameters.

75000

P Bharath reddy

8

PBR

Create Token

12:02 / 22:39

Token Transfer | Etherscan

etherscan.io/tokentxns

Etherscan

All Filters | Search by Address / Txn Hash / Block / Token / Ens

Eth: $2,649.59 (-3.68%) | 116 Gwei

Home | Blockchain | Tokens | Resources | More | Sign In

ERC20 Top Tokens
View ERC20 Transfers
ERC721 Top Tokens
View ERC721 Transfers
ERC1155 Top Tokens
View ERC1155 Transfers New

Token Transfers ERC-20

Featured: Review and revoke dApp access to your tokens with our **Token Approvals tool!**

A total of > 10 M txns found
(Showing the last 10,000 records only)

ge 1 of 200 | Last

Txn Hash	Age	From	To	Value	
0x76b58bbd6617a331b9...	38 secs ago	0x39703410252d6b10cf...	Null Address: 0x000...000	57,237	(WOOL)
0xe6cec9f5b5cf648e5a0...	38 secs ago	0x1392400cf4fe273b6fa...	0x9c9ab2d469d1656842...	477.057139	USD Coin (USDC)
0x1c83c122e28648e6e2...	38 secs ago	StrongBlock: Service	0x4b5057b2c87ec9e7c0...	10	Strong (STRONG)
0x1c83c122e28648e6e2...	38 secs ago	0xb9b6f64234dc3d0c3b...	StrongBlock: Service	10	Strong (STRONG)
0x5595a474dbed9d9220...	38 secs ago	0x7fe788262bb12a8805...	CoinList 2	501.499175	USD Coin (USDC)
0x3d7cb993d2054cf82e...	38 secs ago	Uniswap V2: LOOKS 3	Uniswap V3: Router 2	0.113325248836560462	Wrapped Ethe... (WETH)
0x3d7cb993d2054cf82e...	38 secs ago	tallwesty.eth	Uniswap V2: LOOKS 3	165.553169686199079875	LooksRare To... (LOOKS)
0x166d5de8d71cc15555...	38 secs ago	Null Address: 0x000...000	ggbrokoli.eth	4,755.127943915427948785	WOOL (WOOL)

13:21 / 22:39

javascript:

Non-Fungible (ERC-721) Tokens

etherscan.io/tokens-nft

Etherscan

All Filters | Search by Address / Txn Hash / Block / Token / Ens

Eth: $2,648.88 (-3.71%) | 130 Gwei

Home | Blockchain | Tokens | Resources | More | Sign In

Non-Fungible Token Tracker ERC-721

Non-Fungible Tokens (NFT)

A total of 44,251 ERC-721 Token Contracts found

First | Page 1 of 886 | Last

#	Token	Transfers (24H)	Transfers (3D)
1	Ethereum Name Service (ENS) ENS offers a secure & decentralised way to address resources both on and off the blockchain using simple, human-readable names.	12,819	24,029
2	Invisible Friends	12,184	13,017
3	Morphs	11,521	11,700
4	3Landers	10,718	10,718
5	0xapemfers	10,515	10,540
6	ChillRx	9,385	11,838
7	Imaginary Ones	9,255	9,255
8	ShadesOfYou	9,228	9,505

13:38 / 22:39

Multi-Token (ERC-1155) Tokens

etherscan.io/tokens-nft1155

Etherscan

All Filters | Search by Address / Txn Hash / Block / Token / Ens

Eth: $2,648.88 (-3.71%) | 126 Gwei

Home | Blockchain | Tokens | Resources | More | Sign In

Multi-Token Token Tracker ERC-1155

Multi-Token Tokens

A total of 5,493 ERC-1155 Token Contracts found

First | Page 1 of 110 | Last

#	Token	Transfers (24H)	Transfers (7D)
1	OpenSea Shared Storefront Discover, collect, and sell extraordinary NFTs on the world's first & largest NFT marketplace.	22,020	66,005
2	parallel (LL)	10,896	13,036
3	0xbfc5f30e9da14d9506a0ea1eea71e2bf6bb0c3f9	5,271	5,271
4	0x0546f6d538a2abf964ae4d537a131b226eba9285	2,067	3,404
5	0x207ce3186b13a2855d9ce8fdb56eacc53e84fb4b	1,764	2,683
6	0x17f5655c7d834e4772171f30e7315bbc3221f1ee	1,306	2,418
7	Superlative Artifacts Superlative Secret Society are collectible #NFTs inspired by primary personality traits.	1,166	4,561

13:48 / 22:39

ERC-721 and CryptoKittens

ERC 721 - For Non Fungible Assets

ERC 20 - For Fungible Assets

ERC 721 -> address + tokenID
ERC 20 -> address

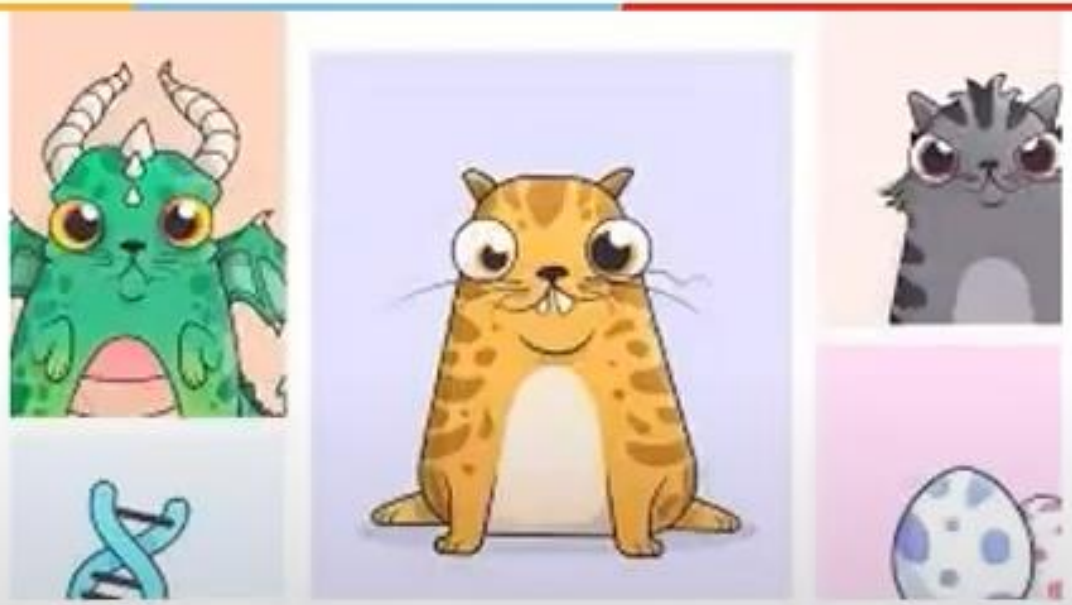
Mandatory Functions in ERC721

- balanceOf
- OwnerOf
- safeTransformFrom
- transferFrom
- Approve
- setApprovalForAll
- getApproved
- isApprovedForAll

Interface ERC721TokenReceiver

This has been created by blockchain, can't be changed by anybody

Creation of NFTs (crypto-collectible) - 3rd most GAS hungry on ETHEREUM at one point



50,000 generation zero crypto kitties!!!

Ethereum – Video Lecture from Youtube

Modern Technology

- Reduce costs
- Remove points of failure
- Preventing censorship
- Transparent

Bittorrent

- First decentralised application
- Developed in 2001
- Designed by Bram Cohen

Blockchain

"A blockchain is a growing list of records, called blocks, that are linked together using cryptography."

- Wikipedia

Bitcoin

- Digital Currency
- Decentralised money
- Blockchain

Vitalik Buterin

- Co-founder of the Bitcoin Magazine
- Came up with the idea of creating a new blockchain Network

Ethereum

- Vitalik Buterin created Ethereum
- Funded by a public crowdsale
- Went live on 30 July 2015
- “Programmable Blockchain”

Ether

- Cryptocurrency
- Only currency accepted in the payment of transaction fees
- "Digital Oil"

Gas is the fee required to successfully conduct a transaction or execute a contract on the Ethereum blockchain platform. Fees are priced in tiny fractions of the cryptocurrency ether (ETH)—denominations called gwei (10^{-9} ETH). Gas is used to pay validators for the resources needed to conduct transactions.

Smart Contracts

"A computer program intended to automatically execute according to specific terms or instructions"

-Exodus

Gas

- Needed to run computations on the blockchain
- Encourages efficient code

Ethereum Virtual Machine

- Runtime environment for transaction execution
- Isolated from the other files

Dapps

- Provide some function or utility to its users
- Operate without human intervention
-

Coins

- Contribute to features of Ethereum
- Follow ERC rules
- ERC-20 standard

DAO

- Decentralized Autonomous Organization
- $50 million of DAO tokens were stolen
- Hard Fork

Crypto Kitties

- A blockchain game on Ethereum
- Ethereum miners increased the gas limit in response to Crypto Kitties

Ethereum 2.0

- EIP 1559
- Phase 0
- Phase 1
- Phase 2

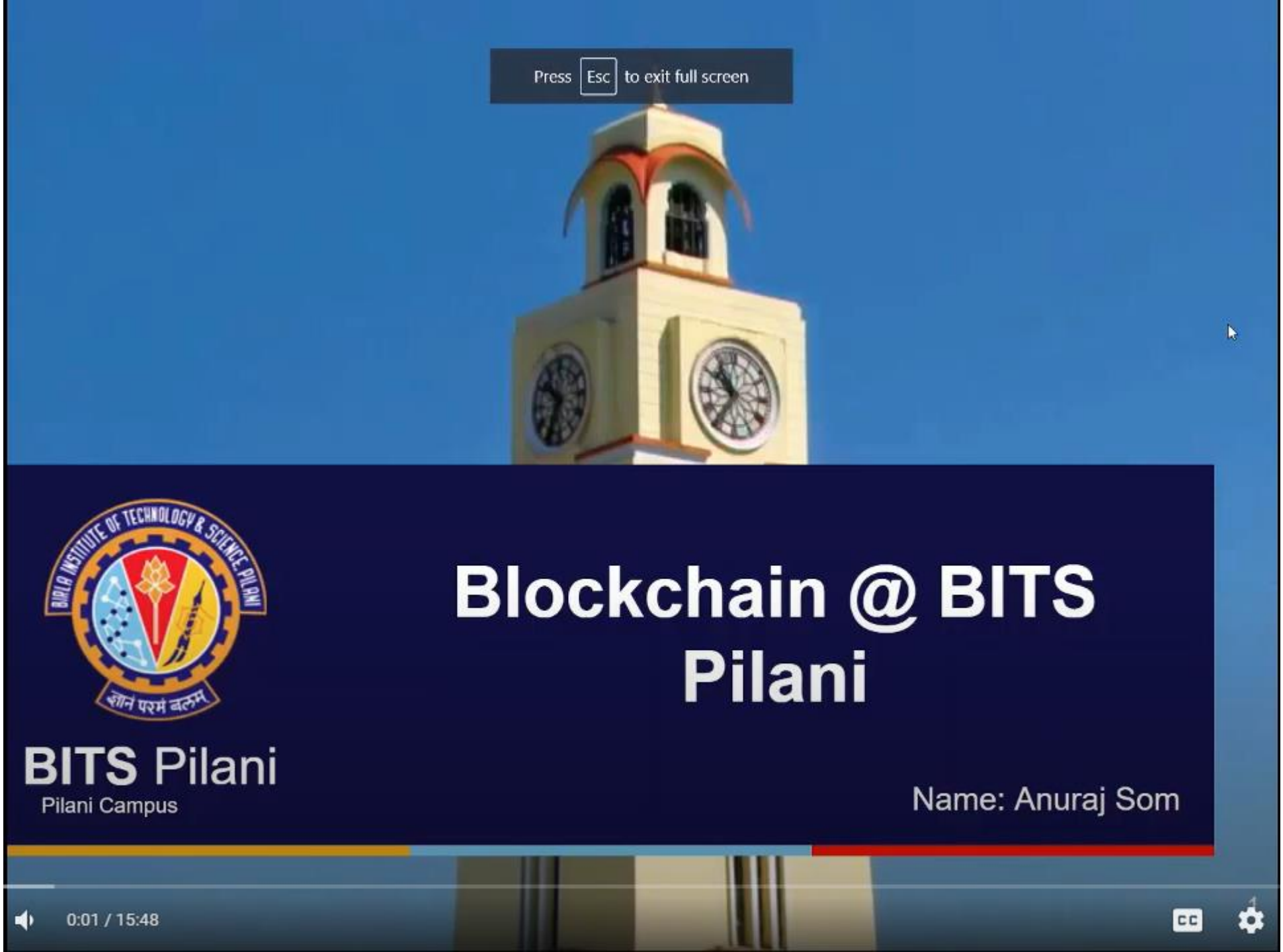
- **The Ethereum Virtual Machine and Gas**
- Discussing gas requires introducing the Ethereum Virtual Machine (EVM). At a high level, the EVM is the environment in which smart contracts are executed on the blockchain. Each node in the Ethereum network runs the Ethereum blockchain, and together they collectively form the EVM — or, the Turing-complete world computer. Within the EVM, smart contracts are executed through a series of operations. Stated another way, a transaction on the Ethereum blockchain can initiate a smart contract, which is comprised of a series of sequential operations — all of which occurs within the EVM.
- On the Ethereum blockchain, each operation (many of which can be combined to create a single unique smart contract or transaction) requires a certain amount of computing energy, or work, to perform. Because miners must use energy to complete these operations, a unit of measurement was created to monitor and compensate miners for the work they spend running transactions and smart contracts. This unit of measurement is called gas. Gas is a unit of measurement unique to the Ethereum blockchain that measures the computational work required to run transactions or smart contracts within the EVM. The more energy required to run an operation (i.e. a more complex piece of code), the more gas is required.
- Gas itself does not “exist.” In other words, it cannot be owned; one cannot have a “gas token.” Rather, the value of each unit of gas is expressed in ETH. For instance, an operation might cost 3 gas, which could be equivalent to 0.00004 ETH. So if gas is measured in ETH, why not just get rid of gas and express the cost of each operation directly in ETH? The price volatility of ether is no secret (in the same January 1–3 timeframe, the price increased 25%). The computational energy needed to perform a specific transaction, however, remains constant. The gas cost of running an “addition” operation on Ethereum, for instance, was the same on January 1 as it was on January 3, regardless of the value of ether.
- The concept of gas, therefore, exists to separate the computational cost of running an operation from the market value of ether. The gas cost (i.e. the energy needed) of an operation remains constant regardless of price volatility. That gas cost is not easily changed; however, how much ether each unit of gas represents is easily changed. Therefore, if the price of ether skyrockets, the network can reduce how much ether each gas represents to keep constant the cost to the person paying for gas.

A Guide to Gas for the Ethereum Blockchain | ConsenSys

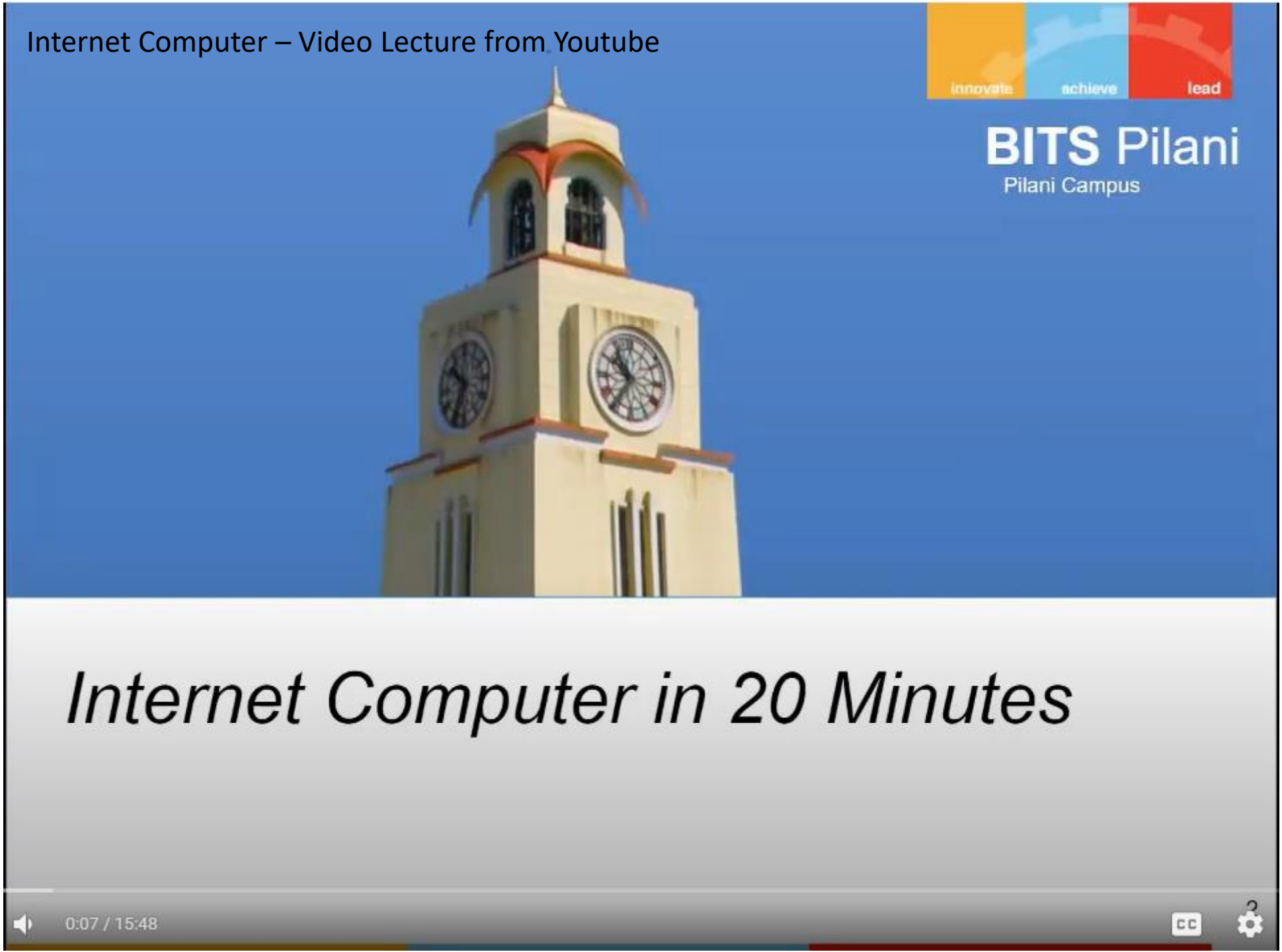
- **Components of Gas**
- Broadly speaking, gas can be split into three concepts: gas cost, gas price, and gas limit:
- ***Gas Cost*** represents the units of gas required to run each operation. The gas cost of each operation on the Ethereum blockchain was predetermined in the yellow paper. For instance, the gas cost of running an “addition” operation is 3 gas, and will remain 3 gas regardless of the USD value of ether. This clarification provides further insight into why we use gas instead of directly associating ether with the cost of running an operation. Whereas the amount of gas needed to run a single operation cannot be easily changed by the network, the price of gas in ether can easily respond to the volatility of ether or to network traffic.
- ***Gas Price*** is the value of a unit of gas in ether. Gas price is measured in “Gwei.” (gwei (10^{-9} ETH)) One Gwei is 1 billion Wei, and a Wei is the smallest unit of ether. Sites such as ethgasstation.info post the average gas price on the network, but users may be willing to set a higher gas price on their transaction to be prioritized by miners. Miners keep the gas (or, more exactly, the ether one pays that represents gas) that a user attaches to a transaction. They will prioritize, therefore, a transaction that has a higher gas price associated with it over other transactions with a lower gas price.
- ***Gas Limit*** is the maximum amount of gas one is willing to spend on a particular transaction. The gas limit can be, and typically is, greater than the actual amount of gas the transaction requires. If a user specifies a gas limit that is too low (i.e. the operations within the transaction collectively require more gas than the user attaches to the transaction), then a miner will complete the transaction until the gas is used up. At that point, the miner would keep the fees (as they spent time and energy on executing as many of the operations as they could), the transaction would fail, and the blockchain would keep a record of the transaction as “failed.” Gas limits exist to protect users and miners both from losing funds (for users) and energy (for miners) from faulty codes or malicious attacks.

- **Why Does Gas Exist?**
- The components of gas, its utility, and potential pitfalls for an inexperienced user bodes the question — why does gas exist in the first place? Speaking broadly, gas exists on the Ethereum blockchain to address three reasons: financial, theoretical, and computational.
- The ***financial*** purpose of gas is to incentivize miners to apply their time and energy towards executing transactions and smart contracts. More complex operations require more computation, and therefore more gas. If a user wishes to have their transaction prioritized, s/he may dictate a higher gas price, therefore likely convincing miners to process that transaction sooner. Gas as compensation for energy will become more crucial after the implementation of proof of stake. As miners will no longer receive ether as a reward for mining a block into existence, financial reward for expending energy on the blockchain will come from processing transactions.
- The ***theoretical*** purpose is a matter of aligning the incentives of participants on the network. Much of blockchain theory discusses how to mitigate harmful or malicious actors in a trustless environment. Gas partially addresses this issue by aligning economic incentives between users. Miners are incentivized to work on the network and users are de-incentivized from acting poorly or writing malicious code as they are putting their own ether (in the form of gas) at risk.
- The ***computational*** reason behind gas goes back to an old, foundational aspect of computing theory — the Halting Problem. The Halting Problem is the issue of determining whether an arbitrary program will stop running or if it will run forever just from looking at the description and the input values. In 1936, Alan Turing determined that it is impossible for any machine to solve the Halting Problem. In the EVM, this means a miner is never able to begin processing a transaction and know 100% that the transaction won't go on forever. With gas — specifically, gas limit — a finite amount of gas is always attached to a transaction. Even if a miner began processing a transaction that was coded to continue indefinitely — either from a bug or an attack on the network — the gas would eventually run out, the transaction would end, and the miner would still be compensated.

A Guide to Gas for the Ethereum Blockchain | ConsenSys


Press Esc to exit full screen
BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्
BITS Pilani
Pilani Campus
Blockchain @ BITS Pilani
Name: Anuraj Som
0:01 / 15:48

Internet Computer – Video Lecture from Youtube



INTERNET COMPUTER - AN INTRODUCTION

The Internet Computer is a decentralized computing network. It is a public blockchain that hosts smart contracts that can run at web speed, can serve the web from cyberspace, run efficiently, and can scale within an environment that has unbounded capacity. It has the capacity to extend the internet to be the world's compute platform.

It is being developed by the Dfinity foundation.

0:09 / 15:48

CURRENT PROBLEMS

- Requirement of Big Tech
- Complexity from having to use proprietary legacy stack
- Insecure applications
- Extremely high spending
- Control of data
- Users might not be sure that they are interacting with smart contracts

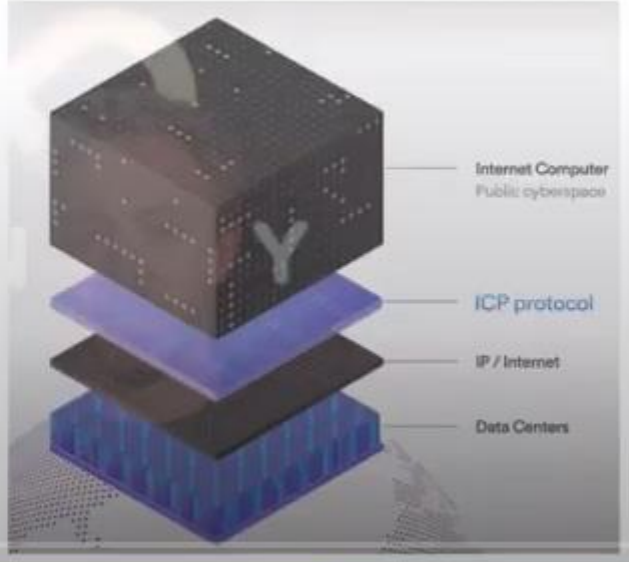
1:13 / 15:48

INTERNET COMPUTER - HOW DOES IT WORK

The Internet Computer is created by the ICP Protocol. It forms the world's first web-speed, web-serving public blockchain network. It can grow in capacity according to demand.

It combines special node machines run in huge numbers by independent parties from independent data centers around the world. Thus it is a blockchain computer which is unstoppable and the code is tamperproof. Even more impressive is that its performance rivals that of the cloud.

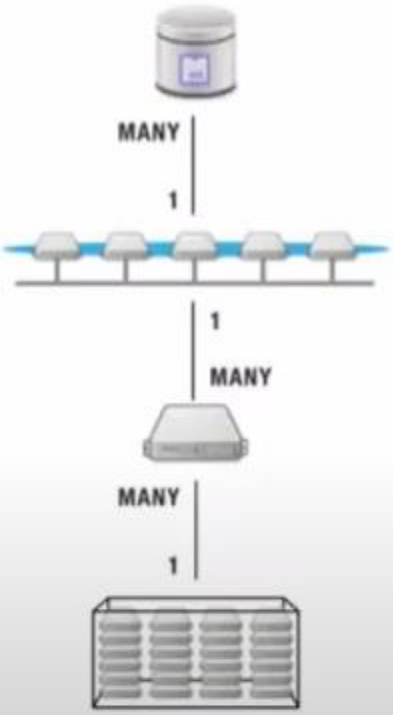
Internet Computer = Network + Compute



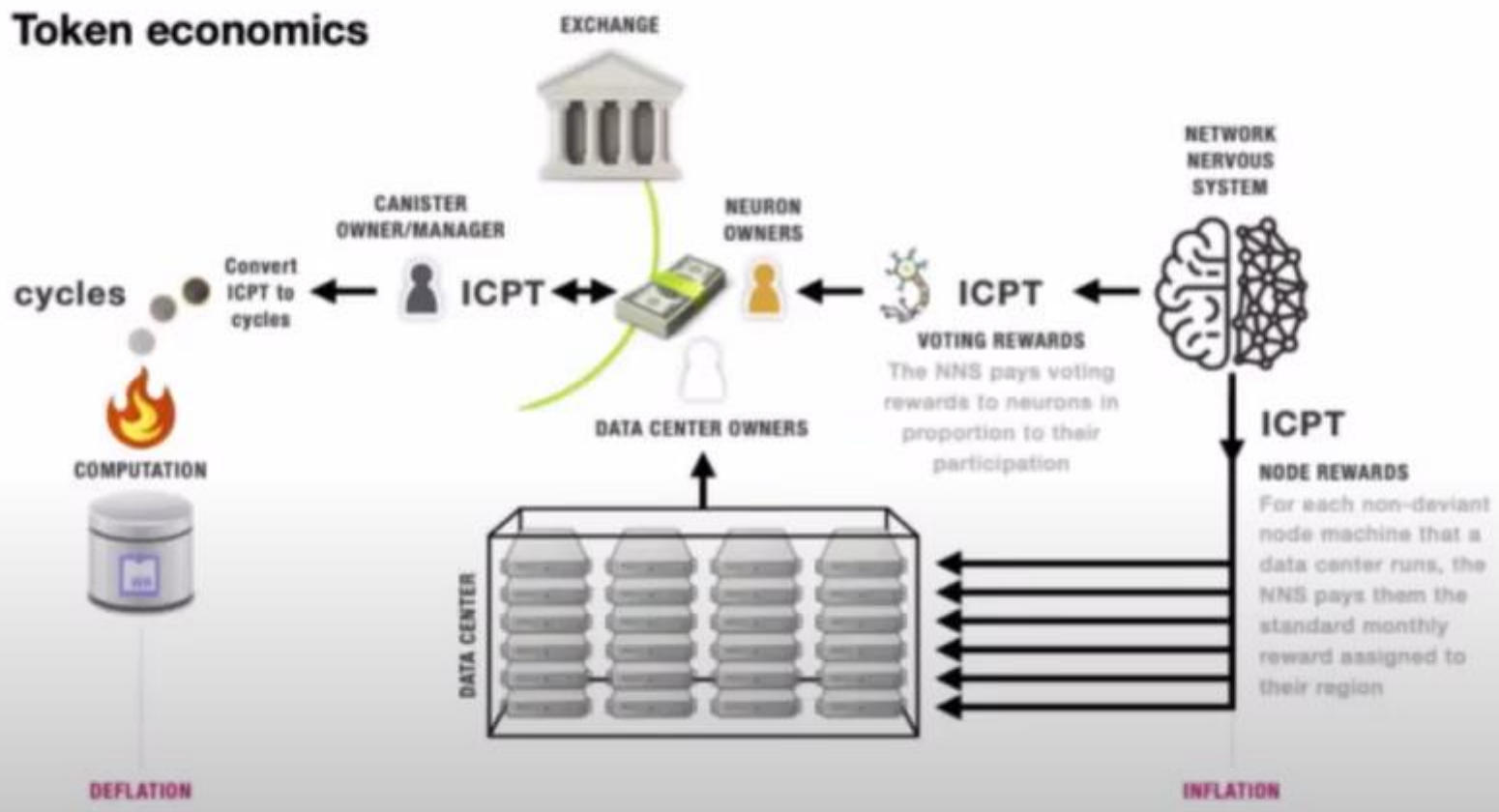
3:11 / 15:48

HIERARCHY OF NETWORK

- Canisters
- Subnets
- Nodes
- Data centers



TOKEN ECONOMICS



6:05 / 15:48

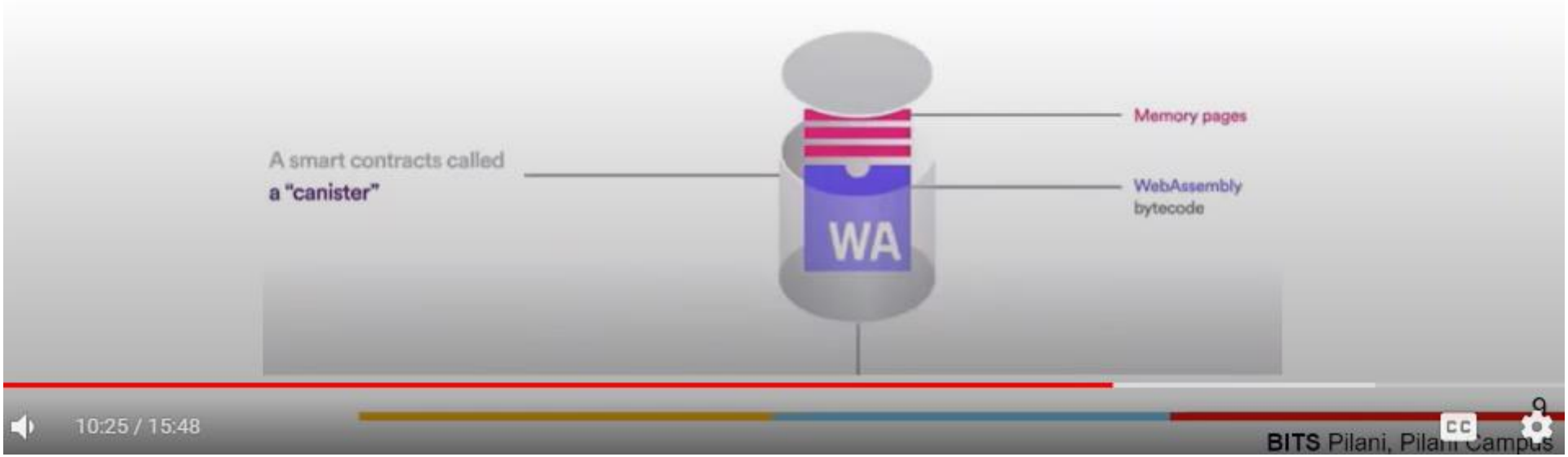
SUBNET

- Used for hosting a distinct subset of the software canisters hosted by the Internet Computer network
- Subnets are tamper-proof and unstoppable
- Transparent to users and software
- NNS can split and merge subnets
- Different types of subsets with different properties:
  - Data
  - System
  - Fiduciary
  - NNS (which cannot be accessed) .

7:33 / 15:48

CANISTER

- Canisters run within dedicated hypervisors and interact with each other via a publicly specified API
- Consists of WebAssembly bytecode created by a high level language
- Functions shared by canisters can be invoked two ways
  - Update call - 2 sec
  - Query call. - Few milli sec
- Canisters can create new canisters



ADVANTAGES

- Can host any number of canister smart contracts efficiently
- Can run them concurrently - Dapps to scale
- Canisters are unstoppable and tamper proof - Firewalls aren't required
- Canisters can serve web content directly to end-users
- Users can interact with blockchain services directly without holding tokens
- Complexity of stack is reduced
- Works at web speed and is powerful
- Combats platform risk
- Data sharing can be managed by transparent open tokenized governing systems

12:56 / 15:48

USES

- Tokenized internet services
- Pan-industry platforms
- DeFi and smart contracts
- Enterprise systems
- Websites

15:23 / 15:48

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्
BITS Pilani
Pilani Campus
Blockchain @ BITS Pilani
Name: Jeeten Kapoor Jain
0:00 / 20:12 • Chapters

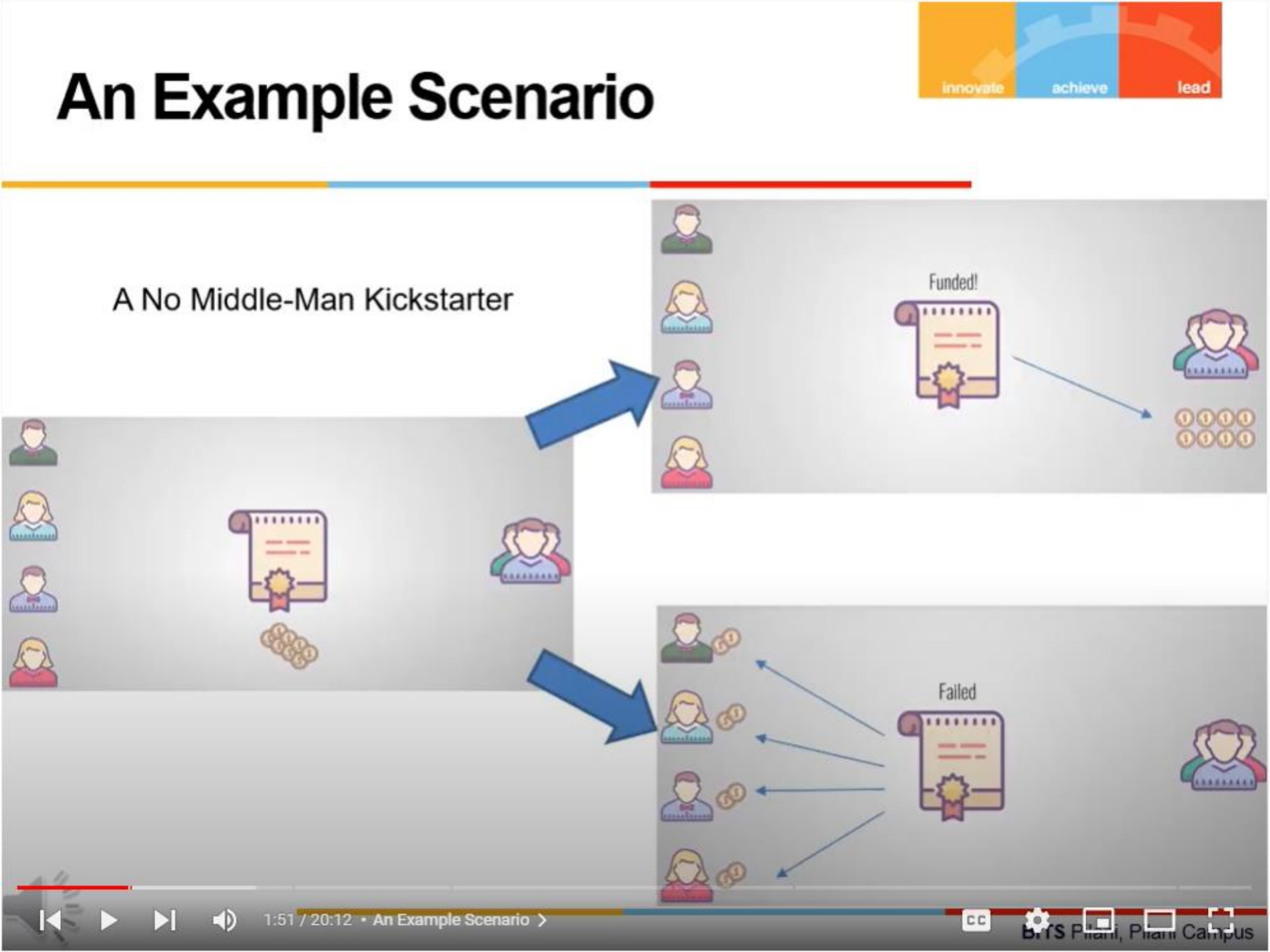
Smart Contracts – Video Lecture from Youtube

Smart Contracts

- Programs/Protocols stored Blockchain
  - because it exists on the blockchain it inherits various security and privacy properties.
- Automatic execution: preprogrammed to when some predetermined conditions is met
- Reduces the need for intermediaries
- Immutability: cannot be changed or updated once they are deployed
- Expanded Blockchain's scope of applications
  - Tokens, DApps, Many more…

0:15 / 20:12 • Chapters
BITS Pilani, Pilani Campus

An Example Scenario



How Smart Contracts Works

innovate achieve lead

How does a SMART CONTRACT WORK?

Pre-Defined Contract

Terms and conditions are agreed by all the parties involved.

Events

Execution of the contract is triggered by an event.

Execution

The smart contract is executed automatically.

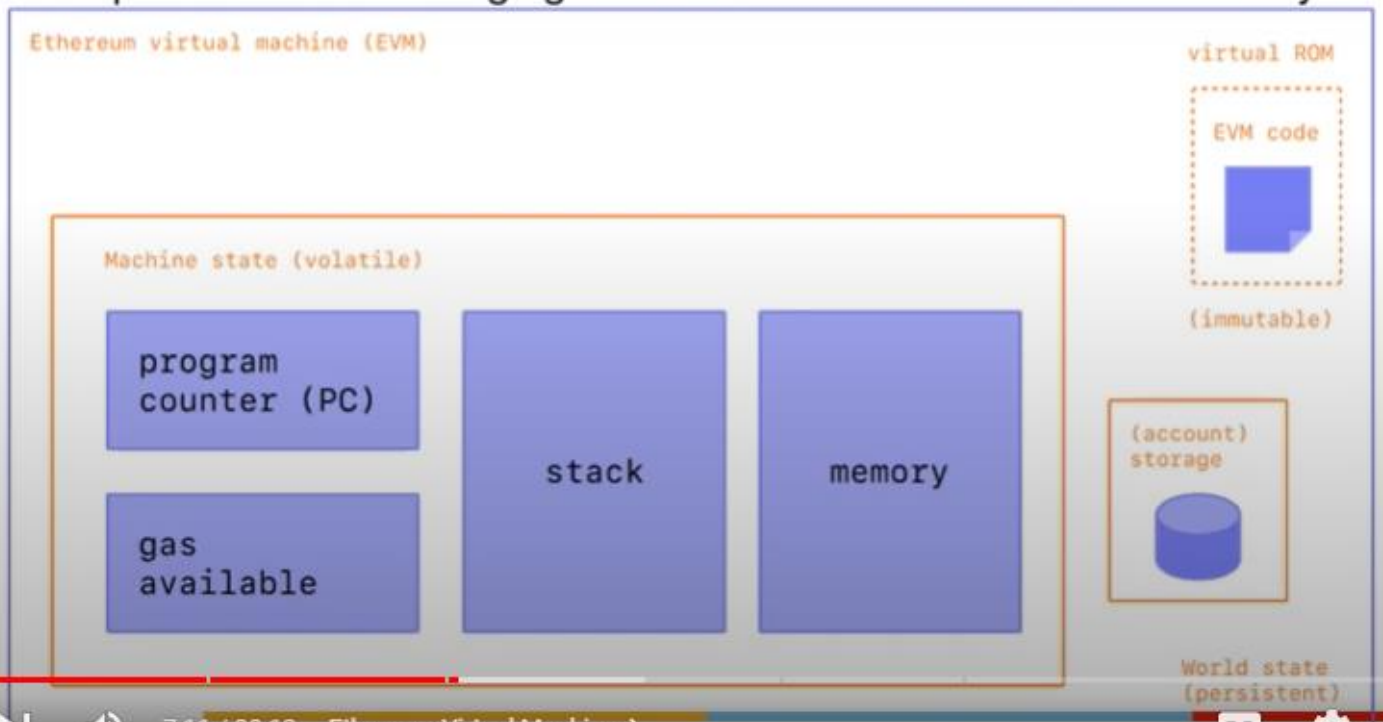
Settlement

All the settlements are executed quickly and eficiently.

4:36 / 20:12 • How Smart Contracts Works
BITS Pilani, Pilani Campus

Ethereum Virtual Machine

- Physical instantiation can't be described
  - exists as one single entity maintained by thousands of connected computers running an Ethereum client
- Ethereum as a distributed state machine
  - The specific rules of changing state from block to block are defined by the EVM



7:11 / 20:12 • Ethereum Virtual Machine
BITS Pilani, Pilani Campus

Smart Contracts on Ethereum

- Smart Contracts are a collection of its code (function) and its data (state)
- They are a type of Ethereum account
  - Like all account it resides at a specific address on the Ethereum blockchain.
  - Like all account they have a balance and can send transactions
- It is Permissionless: Anyone can write a smart contract and deploy it to the network
- Needs certain an amount of gas to deploy and run
  - Deploying a smart contract is technically a transaction, so you need to pay your Gas in the same way

10:45 / 20:12 • Smart Contracts on Ethereum
BITS Pilani, Pilani Campus

What is Gas and why it exists?

- Unit of computational effort required to execute specific operations on the Ethereum network
- The London Upgrade – 5th August 2021
  - better transaction fee estimation
  - generally quicker transaction inclusion
- Every block has a base fee: calculated by network based on demand for block space
- Variable-size blocks: Block has a target size of 15 million gas, but can go up to 30 million gas based on network demand
- Keeps the network secure: every computation executed requires a fee, preventing spamming of network

12:50 / 20:12 • What is Gas and why it exists?
BITS Pilani, Pilani Campus

An Example

Let's say Alice wants to send a transaction to Bob of 1ETH

The fees and refund is calculated as per the formulas below:

$$Total\ Transaction\ fee = gasLimit \times (baseFee\ +\ tip)$$
$$Refund = maxFee - actualFee$$

Alice sets gas limit as 21,000 units and assuming the current base fee as 100 gwei. Alice has included a tip of 10 gwei.

$$21{,}000 \times (100\ +\ 10) = 2{,}310{,}000\ gwei = 0.00231\ ETH$$

No refund in this case!

*As Alice didn't set the optional parameter of maxFeePerGas**

16:06 / 20:12 • What is Gas and why it exists?
BITS Pilani, Pilani Campus

Open Challenges

- Far from perfect: no straight forward way to cater to any requirement for changes in the logic of the code
- No right to remedy
- Bug are visible to all nodes, hence easier to exploit

19:04 / 20:12 • Open Challenges
BITS Pilani, Pilani Campus