**Research on deployment of a token on layer 1 and layer 2 blockchain.**

*Introduction*

Blockchain has emerged as the future technology in the domain of digital transaction due to its way to trace transactions, immutability, cryptography, hashing, decentralised system, consensus mechanism etc.

A blockchain is a distributed ledger that acts as a spreadsheet for the database and is run by a number of nodes around the globe and the data is shared amongst all the nodes.

A block mainly consists of a timestamp, transaction data and hash.

Timestamp - records the right time at which the block was added to the blockchain.

Transaction data - It contains the list of transaction that are contained in a block that can include sender, recipient, amount and some other information.

Hash - Each block has a unique identifier called hash that is created by solving a complex mathematical equation and converts data into a hexadecimal number.

SHA256 is the most commonly used hashing algorithm which produces a 256 bit output.

Etherium uses Keccak256 for hashing.

The first block of a blockchain is called a genesis block. Every block in a blockchain has a block no and nonce

Nonce stands for number only used once that miners use to attempt to generate a valid hash to produce a new block. Its a 32 bit number.

Bitcoin blockchain is the first blockchain made by an anonymous Japanese person named Satoshi Nakamoto in 2008.

Bitcoin works on Proof Of Work(POW) in which miners have to run a race to solve complex problem and the first one to mine the block gets the block reward.

Mining - The process of finding the solution to the blockchain problem is called mining.

Different blockchains use different consensus mechanisms for its smooth tamper proof working.

Consensus - Consensus is the mechanism used to agree on the state of a blockchain.

POW and POS are an example of sybil resistance consensus.

Bitcoin and Etherium both use Nakamoto consensus but bitcoin is a combination of POW and longest chain rule where as ETH is an use POS plus longest chain rule.

In POS miners are known as validators in which nodes are randomly chosen to propose the new block and the rest of the validators validate if the node has proposed the block honestly.

Bitcoin halving - Its a system designed to slow down the production of bitcoin that occurs after every 210000 blocks or roughly after four years by reducing the block reward into half. The initial block reward was 50BTC. As of now 4th halving started in April 2024 and the block reward is reduced to 3.125BTC.

Smart contracts

Smart contracts are a set of codes or instructions that are hosted on a blockchain network. Each smart contract contains some conditions that triggers some outcome.

By running on a decentralised blockchain it allows multiple parties to come and share result in an accurate , timely and tamperproof manner.

In short, they create trust minimise agreements.

Purpose of a smart contract

Immutability

Decentralised

Transparency

Automatically Executes

Everyone has the access to terms of agreement

Some uses of smart contracts:

DeFi - Decentralised finance

DAOs - Decentralised autonomous organisations.

NFTs - Non-Fungible tokens

Gas:

Gas is the computational measurement., The more complex is the transaction more gas is used.

Trxn fee - The amount to be paid to the block producer for processing the transaction.

Gas price - Cost per unit gas used which is specified in Eth or Gwei.

Trxn fee = gas used \*gas price

Private Key:

It is used to sign transactions.

Eliptic curve digital signature algorithm is used to create a public key.

Mnemonic phase >> private key ||| > public address

Hybrid smart contracts:

On chain + off chain agreements

Layer1

It refers to an base layer blockchain implementation such as Bitcoin, Etherium, Solana etc.

Layer2

Layer2 is an application build on top of layer1 or added on top of a blockchain such as chainlink, optimism etc.

There are roughly two types of layer 2

Optimistic rollups

Zero knowledge rollups

*Deploying token on layer1 and layer2 blockchains:*

It includes various steps such as creating a token, deploying smart contracts, bridging, interoperability, security etc.

1. Create a token :

Write a smart contract to create a token on a layer 1 blockchain like etherium and decide it total supply and mint the n number of tokens.

ERC standards - ERC(Etherium request of comments) if using eth compatible environment like ERC20, ERC721, ERC1155.

ERC20 Is used for fungibility in which it is used to exchange an asset of same value and its value cannot be changed.

ERC721 is used for Non Fungible Tokens which defines uniqueness of an asset.

ERC1155 is used for fungible, semi fungible and non fungible tokens.

Create mint and burn functions that allows owner to mint and permanently destroy tokens.

2.Testing on testnet :

Before deploying on main net test your contract on test net.

Check the burn and mint functions on testnet.

Also check if the transferring of tokens works without any error.

3.Deploy on Maine:

Once testing is done you can deploy on main net using etherium or any other layer1 blockchain.

Verify the smart contract on Blockchain explorer.

Choose a layer 2 blockchain and write a similar smart contract for the layer 2 blockchain and use mint and burn functions for the sides of the smart contracts.

Deploying on layer2 will decrease transaction fee and increase scalability.

4.Bridging and Interoperability:

bridging allows two blockchain to interact with each other and if N tokens are mint and locked on L1 it will produce X no of tokens on L2 of the same amount as of N tokens on L1.

Cross-Blockchain is a concept seeking to enable Interoperability between two blockchain networks.

There are two key challenges while doing the above:

How can the network nodes trust the authenticity of cross-blockchain data?

What are underlying security assumptions?

General assumptions

1 Underlying networks are secure with a concept of transaction finality within finite time, after which the transactions cannot be rolled back

2 We loosely use ‘value’ as the generic term to represent the cryptographic object that the blockchain carries.

3 Security aspects such as double spending and 51% attack of cross-blockchain systems are addressed by the integration protocol

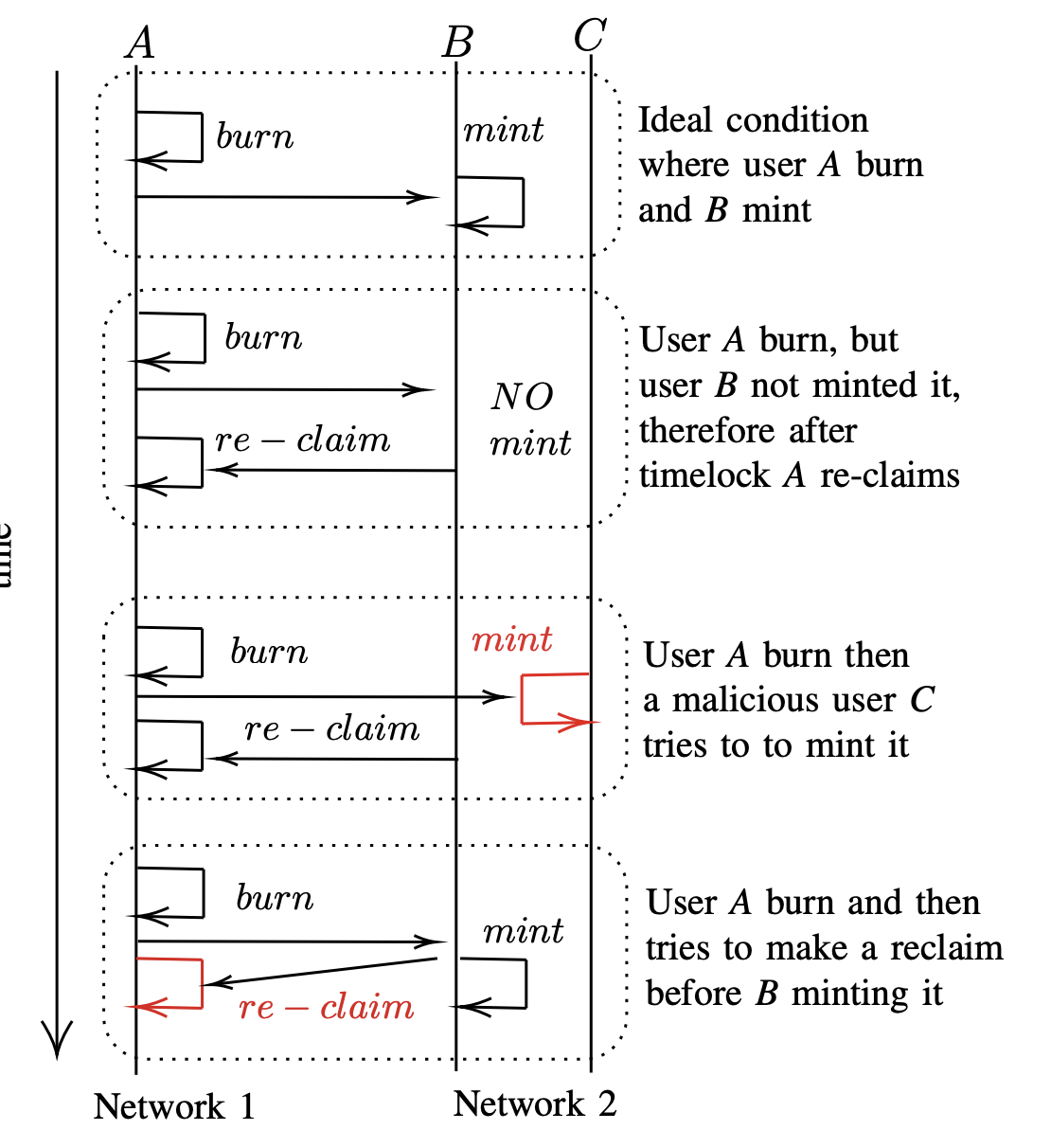
4 We do not consider the semantics of data and exchange rate between two different tokens.

In order to implement it the value representation on one blockchain needs to be locked or removed to represent the same unit of value on the other network.

That is if n tokens value is transferred from network N1 to network N2, the corresponding value of n tokens on N1 must be decreased, and an agreed value of N2 must be increased.This process is achieved by Protocols such as atomic swap, lock/unlock or burn/mint process.

Cross-blockchain allows transfer of assets to choice of network. The asset can be seen as a digital representation of some value in a blockchain.Assets are generally divided into. Fungible and non-fungible.

PROTOCOL:



D. Our modelling approach The following assumptions have been made while designing the models: • All users are online and connected to each other thus know if specific transactions are confirmed.

• Existing nodes will not leave the network and no new nodes will join the network.

• All mining nodes have the same weight to server as validator.

• Blockchain environment and associated functions are not part of our models.

A private key symbolizes the ownership of this asset in the network. A transfer is a process of altering the ownership of an asset within a network. A cross-blockchain transfer moves a user’s asset into a different position and shifts its value into a different blockchain network

**Challenges:**

Definition 1 (Cross-Blockchain Protocol): A cross-blockchain protocol aims to synchronise parts of ledgers on N1 and N2, both of which are inherently trusted to operate correctly.

Definition 2 (Integration): An integration system that helps the consensus participants.

Definition 3 (Atomicity): The transfer operation should only execute one outcome, either the transfer succeeds and the asset is transferred to the recipient; or it is fails and the asset returns to the sender.

Definition 4 (Asset and Coin): We define asset v and coin c as digital representation of tradable objects available on a blockchain, where c represents native token of the system and v represents token created on the system through a defined protocol.

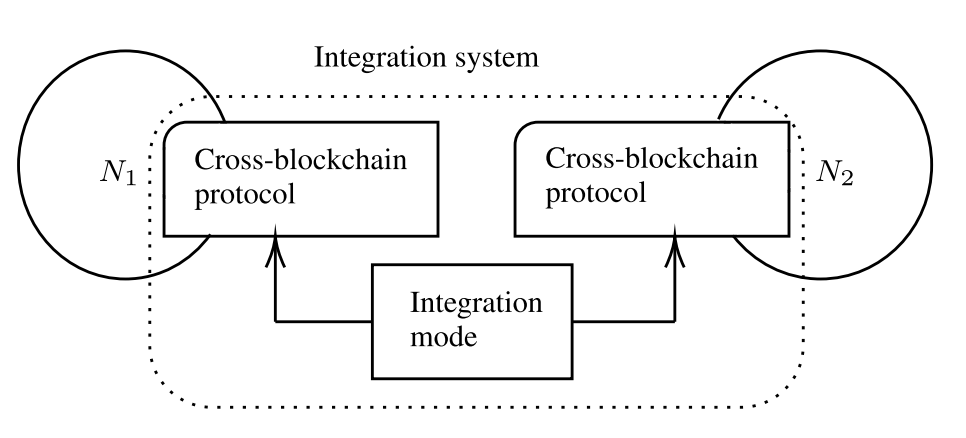
Definition 5 (Cross-Blockchain Trade): Cross-blockchain trade refers to the exchange of asset or transfer of its value between users in different blockchain networks.

Definition 6 (Transaction Finality): Transaction finality refers to the confirmation that a transaction is permanently accepted by the network. As a result it is impossible to alter or

Revert a transaction.

Definition 7 (Degree of Decentralisation): The degree of decentralisation (DD) is defined as the proportion of the total number of nodes against the number of validating nodes in the distributed network. Let n represent the number of nodes and x representing the validating node then DD is calculated by:

DD = number of validating nodes (x) / total number of nodes (n)



Security Issues in Integration:

Security Difference: There must be a difference in the level of security that the various blockchain networks possess. Relatively, if one network is weak then the strong one is also affected when both are combined.

Weakest Link: The overall security of the integration depends with the security of the lowest link in the system. It makes single integration node teeth a very high risk as the break can jeopardise the whole transaction.

Lazy Node: Some of the nodes may act improperly or even corrupt and thus the wrong transaction may be accepted if they don’t validate data correctly.

Decentralisation Degree (DD): Its level is important, however it should be decentralised in the integration system. There is, however, the need to strike a balance between decentralisation and performance.

Full vs. Partial Verification: There are two types of transaction verifications – full-checking, that involves checking every detail in a given transaction, and selective checking, that only checks certain details in a given transaction. It is more secure to perform full verification at times but it is not very feasible.

Cross-Blockchain Transaction Liveness: It must be noted that the system has to finalise such inter-network transactions quickly, and there must be contingency measures in the event of failures.

Cross-Blockchain Integration Modes:

Direct Integration Mode:

Some of the nodes in a network (N1) have to rely on a light client of another separate network (N2).This method entails archiving information needed to prove transactions and the state of information.

However, it has the weaknesses of scalability problems and is a single point of failure.

Third-Party Integration Mode:

Interoperability is achieved through an independent and neutral third party such as a federation of validators.This third party certifies events on one network and authenticates these on the other, thus making correct transactions.

Bridge Integration Mode:

Bridges can be described as intermediaries which connect a variety of blockchain systems.

They employ gateway node for the communications and computations with other networks for reaching out for external data.

Types of gateways include the ones that are incorporated into user’s wallets and the ones that run on the third-party servers.

Connector Integration Mode:

The networks are connected by an integration hub and are, therefore, a ‘network of networks’.Activities and dispatching of messages occur at the hub, of or across the sidechains or even between the linked portions of the network.

Other Modes:

It also connects through custom-built interfaces with off-chain data sources such as oracles or APIs.

These systems collect, parse, and assert external data but data authenticity is a big issue here.

Atomic Swap Protocol:

Enables the swapping of tokens belonging to two different parties without requiring intermediary which is achieved through a series of transactions between the two parties.

Tokens are ‘‘secured’’ by a hash time lock contract (HTLC) from the moment of exchange and are released only when both transaction parties meet certain requirements.

It is efficient only for token exchange to one counterparty at a time and doesn’t support token transfers in general.

Lock and Unlock Protocol:

Tokens are remain on one network and an equal value is released at another network.

It was called the ‘peg system’ and is widely adopted to maintain the initial token while utilising it for a short time in another network temporarily stabilising its value.

Locked token is used as collateral while the unlocked token is simply called the “wrapped” token.

Burn and Mint Protocol:

Tokens are sent to a specific network and are burnt while an equivalent number of tokens is generated in another network.

The burn process entails the use of tokens in such a way that they cannot be spent and repeated anywhere else by being sent to an unknown or a one-way address.

This makes sure that the token is burnt to ashes before we move value to another network at the completion of transactions.

Cross-Blockchain Message Protocol:

Is a means through which messages can be used to enable the exchange of data between different blockchain networks.

Requests installation of like data structures, messaging protocols and security infrastructure in both topological layers of the Networks.

This protocol is required for the scenarios where blockchains have to interact with others, which is called IBC or Cross Chain Interoperability protocol.

ChainLink is an Oracle-enabled decentralised computing platform that is popular for transferring both, data and tangible value.

from any existing systems, or any private or public blockchain.

Wormhole is also an interoperability for multichain applications that is secure and open source.

5. Audit Contracts: Recommend your contracts to auditors who will examine your contracts and inform you of their security and defects tokens across networks.

6.Deploy on Target Networks: After you are done with this, deploy your token contracts on the Layer 1 and Layer 2 networks accordingly.

Announce Deployment: Notify your community about the deployment of your tokens on all the networks and share with them the information how they will be able to interact with tokens across different networks.

References:

Google

Google Scholar

ChatGPT

Phind

Patrick Collins YouTube channel

<https://smallake.kr/wp-content/uploads/2022/11/OA_Pillai_2022_Cross_blockchain_technology_Integration_framework_and.pdf>

https://www.researchgate.net/profile/Babu-Pillai-2/publication/361388545\_Formal\_Verification\_of\_the\_Burn-to-Claim\_Protocol\_for\_Blockchain\_Interoperability/links/62ad727a23f3283e3af090c1/Formal-Verification-of-the-Burn-to-Claim-Protocol-for-Blockchain-Interoperability.pdf