Article

An Approach for Data Privacy Management for Banking Using Consortium Blockchain

Shady Thabet [*], **Hanan Fahmy** [**] **and Sayed Abdel Gaber**[**]

Department of Information Systems, Helwan University, Cairo, Egypt
* Correspondence: shady.thabet11@nbe.com.eg

Abstract**:** Banking sectors commit modern working frameworks and models smooth development based on decentralization with keeping money confront in unused ranges and differing activities.

Consortium Blockchain Privacy becomes a major concern and the challenge of Most of banking sectors.

Development without being hampered being a major concern it can store confirmed, Data privacy includes assuring protection for both insider ad outsider threats therefore access control of Ring signature could help to secure Privacy of inside and outside threats by secure process by RSBAC using CIA triad privacy Confidentiality, Availability, Integrity. This paper proposes a ring signature-based on access control mechanism for determining who a user is and then regulating that person's access to and use of a system's resources. In a nutshell, access control restricts who has access to a system. It also restricts access to system resources to users who have been identified as having the necessary privileges and permissions.

The proposed paradigm satisfies the needs of both workflow and non-workflow systems in an enterprise setting. The traits of the conditional purposes, roles, responsibilities, and policies provide the foundation for it. It ensures that internal risks such as database administrators are protected.

Finally, it provides the necessary protection in the event that the data is published.

Keywords: Consortium Blockchain; Ring signature; Blockchain privacy; Blockchain security; Access Control; Blockchain big data

1. INTRODUCTION

The Blockchain technology may be a crucial development in the fight against fake money competition. It is regarded as the quick outlet for quick, large-scale keeping money operations that are secured to open up untapped markets for financial development and everyday monetary consideration, enabling its smooth expansion into untapped markets and diverse activities. When the ability to save verified, permanent information by self-executing innovation becomes a key issue, it will probably lead to the reduction of compliance offices.

From unused on time trade that motivated us to guarantee securing protection development without being hindered. That's unfortunate for representatives, but automation might replace this expensive, error-prone detailing technique. With the use of a decentralized block chain network,

This consensus-based decentralized database can store transactional data utilizing a new type of ledger technology called a decentralized ledger tracking digital assets on a P2P network. Practically identical copies of the Blockchain are included in every participant's copy.

Among the Blockchain promising applications are network monitoring and security services counting authentication, confidentiality, protection, integrity, and provenance. Currently, these services are given by trusted third-party brokers or using wasteful conveyed approaches. As a result, security is a major challenge for current applications.

Blockchain technology can offer security guarantees that address several common problems in addition to offering a fully communicated, provably secure, and agreed-upon solution.

There are there categories of Blockchain Figure [1], private, public, and consortium. Consortium combines private and public Blockchain.

Blockchain is a partially decentralized network that allows data and transactions to be either open source or private depending on the authority of pre-approved participants rather than giving a single miner or bank complete control over the verification and validation of transactions [1].

Consortium Blockchain Distributed ledger which not only in a single machine its combination of multiple grid machines or computers or servers its over decentralized network that Anyone can read and write in Public Ledger as it not controlled by any read or write permission.

Blockchain Technology for Financial industry Banks in a face fierce competition from new online services for new businesses challenges to provide easy funds exchange and transfer based on encrypted from here banks rely exactly on Blockchain's as a common ground, it's a New Technologies Deepens the competition in the banking sector. [2]

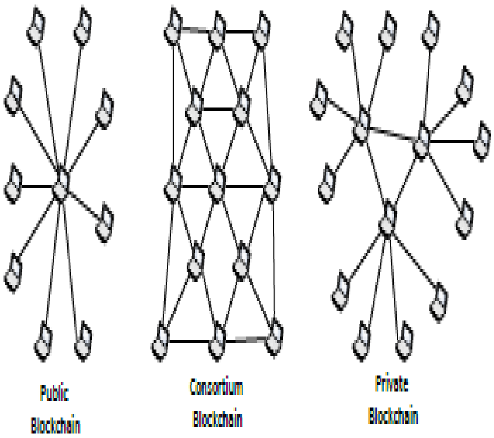


Figure 1: Decentralized network [2].

Consortium Blockchain Distributed ledger which not only in a single machine its combination of multiple grid machines or computers or servers its over decentralized network that Anyone can read and write in Public Ledger as it not controlled by any read or write permission.

Banking sector are starting to store information on their Consortium Blockchain using market technologies to gather customer's relevant data.

These personal details could relate to clients, credit card numbers from private institutions, financial services, etc., as other information services like person experience. Phishing crimes have been committed, and several successful hacking attempts and disclosures of personal information have made many online users fearful of their privacy and vulnerable to abuse. The risk of data breach, which includes all shaky supply chains that pose a risk to human life and property, has come into focus.

In order to do their jobs, banks must follow new operating models that involve limiting access to resources through access control decisions, legal centralization, laws defined by security policy, and evaluation of the privacy and security of Blockchain to assure full compliance with client information and compliance for all institutions employing Blockchain technology. [1]

So, Blockchain revolution must therefore combat Blockchain privacy by utilizing access control models, it is possible to conduct secure transactions without obtaining identification information from credible sources when privacy issues grow. It is determined that all these models' functionality must be improved in order to include some dynamic properties that will reduce their complication.

Blockchain modules that control transactions are available in Blockchain this module that control transactions are available in Blockchain such as Decentralized Ledger, Smart Contract, Hard Fork, Mining is the process of processing the pending transaction by adding an additional Block into the Blockchain through a mathematical POW scenario which require to resolve a mathematical problem to verify the work and get rewarded for achieving this.
Miners may be controlled by a person or group via a computer or server.

1-2 Blockchain features.

- Smart contracts: a controlled term using Blockchain technology used to describe program code in capable executing, and enforcing the negotiation and agreement& Regulations in automated process recorded in a computer language as an instruction of bank policy or central bank regulation's. [3]
- Hard Fork: Forcing method to update core software or business logic of Blockchain & to recover the Blockchain from any damage or cyber-attacks or transaction crimes a malicious user may illegally access private transaction data that significant attention because including transaction amount, account information, and balance due to public Blockchain is transparent and open [3]

1-3Advantages of Blockchain

- Group compliance can reduce fraud by strengthening its regulatory compliance example: after record stored in the ledger, it cannot only before a consensus.
- Consortium Blockchain Build on decentralized networks, Blockchain Technology data would be complete accurate on time
- All transactions will have timestamped using a cryptographic hash code, with unique signature 64-digit alpha-numeric it is recorded corresponding for every single transaction.
- Blockchain Technology Not managed by only control center that not and there's no single point of failure regularly.
- Blockchain is using technology peer-to-peer transaction which supports a decentralized concept.
- Using Smart Contracts in Blockchain Technology gives it self-executed code commands which executed and stored on Blockchain.
- All transactions are under shared ledger& Control of it by many control center that makes it transparent by any counterpart. [6]

1-4 Challenges and Barriers of Blockchain

- Services costs are high and time critical is massive transaction it decrease by increasing number of miners /banks/ controls.

- Blockchain have potential issue in the Blockchain and its ledger implementation the signatures that do not provide guarantee of the owner, hacker can modify and broadcasting a transaction again which can have broken the transaction confirmation.
- Required amount of power resources.
- Blockchain technology and its solutions require changes of existing legacy systems or reengineering it in order to incorporate.
- It is new technology might lead to transformation or changes in organization structure, process, strategy, or culture. [7]

2. BACKGROUND

Ring signatures are produced using a single private key and a collection of dispersed public keys. The whole set of open keys, including the one that compares to the current private key, is frequently referred to as a Ring. A person verifying the signature would not be able to determine which private key from the Ring was used to send the signature. Bunch signatures the original name for ring signatures since they are used to demonstrate that an underwriter had a location where they could congregate without really identifying the signer. They will assist in making money streams untraceable in the context of exchanges. Plans for rings with signatures can display several characteristics that are beneficial for improving confidential transactions.

Anonymity an observer should not be able to determine the characteristics of the message's true follow.

In a sense, the private key that is being used matches one of the open keys inside the Ring. [5]

Link ability will become connected and the trickery will be exposed if a private key is used to sign two different messages.

This property will offer assistance avoiding double-spending attacks. Excludability.

a Ring part whose open key has been utilized twice in two Ring signatures, but is not the genuine underwriter for both, will not be connected Figure 2.

Ring signature is a type of cryptography technique[11] , digital signature can be performed by any member or bank by provide an anon mount signature without revealing the official signed and this signed cannot revoked because the group using Ring signature in consortium Blockchain can be provided as Ring consist of account key and number of public keys which seems Like output to pull its into Blockchain with distributed in triangular matter without no outside observation which meets security advantage of private Blockchain and accountability to access management module with end to end tokenization to enhancement consortium Blockchain elaborates [10].

The proposed adding advantage of following zero knowledge, Ring signature use zero-knowledge for complements to creative Varity ensure there replacing effective automatically with increasing Blockchain throughout and scalability [9].

The Blockchain literature explains exactly the Blockchain security proof and contrasts it with the Priceline security proof as follows. Customers remain "anonymous" despite the fact that exchanges are public as long as public keys are not connected to people's off-chain personas. This detachment of off-chain characters from exchanges and virtual exchanges offers[32].

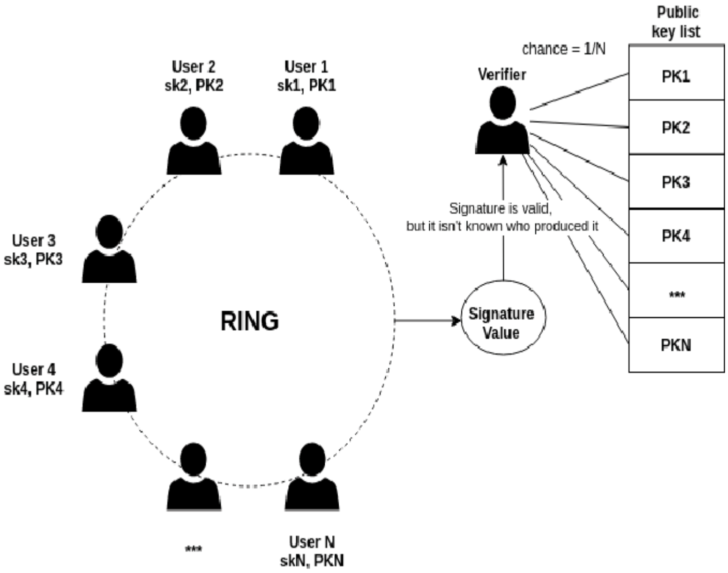
Pseudonymity is a feature that Blockchain users have access to.

There are several benefits touted by an open Blockchain, such as the ability to trace assets through it and the ability for collectors to verify that they are buying authentic goods thanks to certifications disseminated on the Blockchain. [8] Some people believe that the open nature of exchanges poses a threat to fungibility and is in conflict with the something else "pseudonymous" nature of Blockchain.

It helps customers maintain control over their information and consults with them using end-to-end encryption while sharing complex documents with security experts to permit individuals and restrict others by encrypting data into private areas, which may address security issues with public Blockchain in banks.

Ring signatures are a cryptographic mechanism that was initially formalized for the purpose of enabling any member of a set or group to approve a signature without disclosing the identities of the signers on their behalf.

It provides group members with a level of anonymity that is not provided by other digital signature protocols. [4]



(Figure 2: Ring signature cryptography protocol [12])

Ring signatures are a cryptographic mechanism that was initially formalized for the purpose of enabling any member of a set or group to approve a signature without exposing the identification of the signers on their behalf. [33].

It enables group members with a level of anonymity that is not provided by other digital signature protocols. A user can sign to a message or request transfer using the ring signatures scenario. Ring money is assigned to the Ring of given signers for issuing purposes (which could be a bank or financial institution of which the users are members), without disclosing which member of the Ring really generated the money. [14].

Ring signatures among this all-encompassing notion of Ring's ad-hoc identification methods to the notion of signature groups the anonymity of a signer may be withdrawn on group signatures that have the additional access feature by a group manager or higher level.

Ring signatures provide more efficient group management without the need for coordination from numerous other users or miners, which might occasionally be necessary when it comes to the generation of public keys. which support Ring signatures to naturally lends variety of modules in applications which have been suggested

A primary requirement of any bank's Blockchain platform will be how to safeguard all resources and data against unauthorized access or appropriate access modifications. It will also need to provide CIA concept integrity, while also guaranteeing time availability to authenticated users to prevent denial-of-service attacks.

Enforcing confidentiality requirements for every access to a Blockchain with full control and only.

Ring signature to begin with recommended by Rivest et al, who highlighted the RST conspiracy in their paper from 2001, In response to the limitations of group signature, ring signature was developed. In particular, they provide genuinely interested clients with "unconditional anonymity" and are created without the need for a convoluted setup procedure or a group director. Clients are generally required to be a part of an existing open key framework.

Ring Signature Merging Plans (RSMS) enable different Blockchain users to create groups and signatures promptly without requiring any additional trust, at the cost of minimally added processing time. In case the underwriter has knowledge of a few mysterious facts, most typically a private key comparing to one of the open keys within the Ring, the Ring signature are generated in a way that the Ring can as it re be "completed," and thus verified accurately.

For the purposes of the signature generation computation, a number is generated at random for each of the other open keys in the Ring. The endorser then uses the information from their own private key, or other 'trapdoor information,' to close the Ring. Ring if you know any mysterious data that the underwriter might be aware of, typically a private key to a key that is already open inside the Ring. For the purposes of the signature generation computation, a number is generated at random for each of the other open keys in the Ring. The endorser then uses the information from their own private key, or other 'trapdoor information,' to close the Ring. By hiding exchanges inside a collection of other exchanges, ring marks give customers a sense of anonymity. If many customers are making contributions to the Ring in amounts that are extremely comparable to one another, the Ring is said to have excellent liquidity. This means that exchanges can occur quickly and can be successfully combined, with a strong resistance to attempted blending examination attacks.
By hiding exchanges inside a collection of others' exchanges, you can give customers a certain level of anonymity. If a large number of clients are making relatively equal contributions to the Ring, the Ring is said to have excellent liquidity. This means that exchanges can occur quickly and can be successfully combined, with a strong resistance to attempted blending examination assaults [30] [31].
Requests for approved access are granted. Access control is the term for this procedure. [13].
the data publication model face of the privacy-preserving model
To defend against external risks for contacting the privacy protection, many alternative access control models reestablished.
workflow and non-workflow systems used in banking operations [29].
focused on the Ring access matrix in order to guarantee that the appropriate access is given to the appropriate person at the appropriate time. Without requiring any explicit identification, ring signatures can be used to give a member of a particular group of user's access to a resource.

Prior to the most recent work, assuming that authorized users always sign with safe to the Rings made solely of approved-generated public keys that are limited use and not secure in the latter case since it is limited use since Rings are constructed.

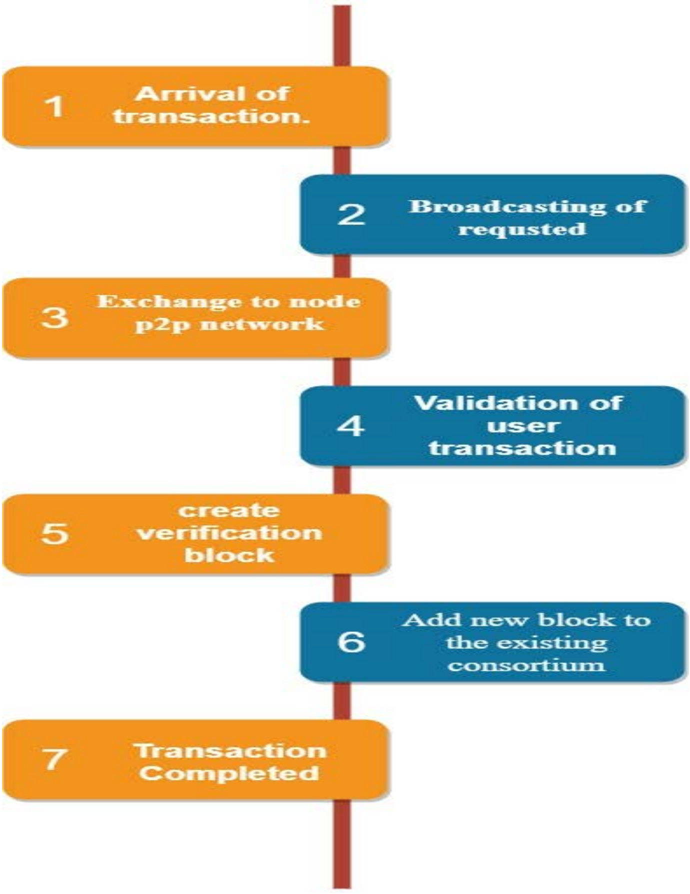
Traditional access control involves a manager's ability to delegate administrative responsibility to others, which poses a security risk and makes access control lists (ACLs) challenging to maintain when user numbers rise. [16].

Ring signature scheme-related work in general has problems. The study article that inspired us to employ the access matrix module
inside some of it, when there is no central group manager to deal with the authorizers TRBAC, PBFW, and PBAC are a few of the platforms it uses.

doi:10.20944/preprints202209.0413.v1

T-RBAC: centralized access matrix control model, which is an improvement on the previous RBAC model and includes elements of user relationships with permission-granting roles and tasks but is difficult to categories,.

PBAC: controlling user access to one or more platforms based on a combination of business roles and policies Users should only be granted a certain amount of access in each role. [17] [20].
PBFW: Flexible Policy Based Access Control Model for Workflow Management Systems which give us flexibility in delegation through Ring signature [18].


1 Arrival of transaction.
2 Broadcasting of requsted
3 Exchange to node p2p network
4 Validation of user transaction
5 create verification block
6 Add new block to the existing consortium
7 Transaction Completed

(Figure 3: Workflow of Blockchain[23])

3. Proposed approach

3.1 Outline This paper focuses on one aspect of This paper focuses on one aspect of banking.

Explain the most recent findings for each proposed Ring Signature Mechanism while introducing a novel idea that is compatible with the consortium's Blockchain & Ring Signature Library and proposed Access control scheme. examine the privacy and security features provided by this scheme, evaluate its effectiveness against other widely used methods, and discuss the need to enhance such models and functionality by introducing dynamic features and to simplify the complexity proposed for privacy on the consortium Blockchain.

(Table 1: Proposed approach)

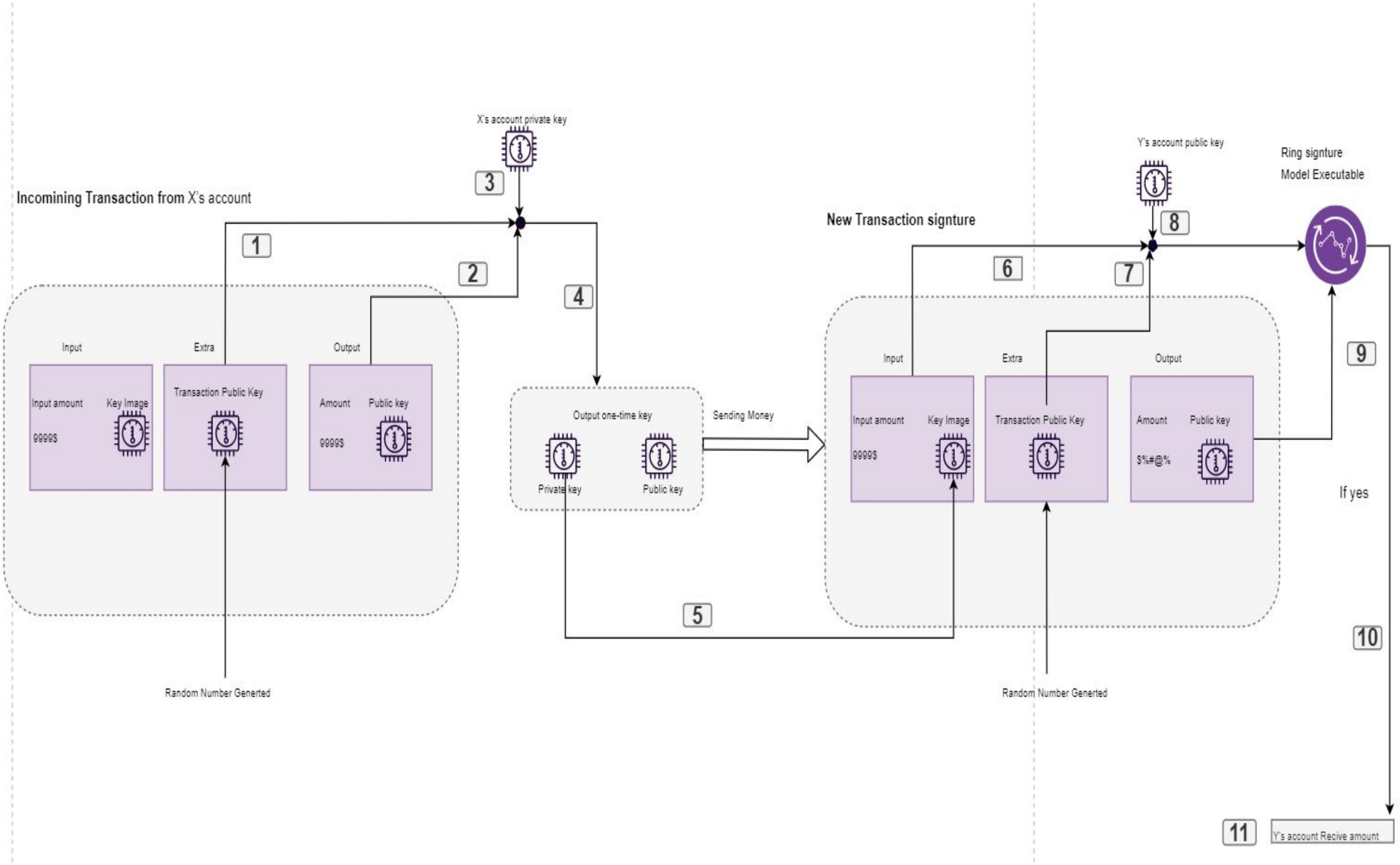
Features	PBFW	TRBAC	CPBAC	Proposed approach (RSBAC)
Task dependency	Exist	Exist	X	Exist
Dynamic permission management	Exist	Exist	X	Exist
Using data conditionally	X	X	Exist	Exist
Dynamic separation of duty	Exist	X	X	Exist
Scope inheritance	X	Exist	X	Exist
administrator protection	X	X	X	Exist
Protection when publishing	X	X	X	Exist

By providing appropriate director dispersion and assignment scope, both user-role and permission-role administration can achieve Blockchain decentralized administration.

The Workflow Security diagram summarizes the security of the workflows as verification, authorization, get access to control, review, information security, information acuity, non-repudiation, security administration, and organization Figure 3.

This proposed access matrix model supports space to hierarchy inheritance utilizing dynamic authorization with decentralized management and Appling Separation of duty [20], with assurance when information are distributed and Protection Protecting of it within the stages Namelessness, unforgeability, Dishonest[21]. Anonymity it is advantage of searching for a particular identifying accurately the person that authorize he signature.

Unforgeability authorizer without a key has no more than a destitute likelihood of authorize a signature that confirms correctly. Collusion resistance Dishonest authorizer within the gather cannot fail by collude to authorize a signature which can confirm as another’s signature confirmation calculation offer soundness and rightness beneath the signature.



(Figure 4: Proposed workflow of Blockchain)

Role: defined a job within bank/organization associated with its activities.

Example, in bank X may have Manager role, Teller role and Customer Services Role. [Figure 4]

Session: defined as the relation between user and activate permission in roles the user enrolled to.

User: refers to employees who can access the Blockchain platform data and resource. It maybe person or service account of application program.

- Domain: are system boundary access permission or roles-scope.
- Task: Tasks are activities or business banking processes.
- Operation: there are many different banking operations like approve, reject, add, delete, modify…etc.
- Authorization: like a Policies which are enforced by the system, sign not assigned to the same user.

Ring signature Based Access Control (RSBAC) design for proposed to simpler access management in consortium Blockchain.

Include and safeguard of properties that take into account client characteristics, asset qualities, and protest properties according to user requirements.

Uniqueness or representations are extracted by RSBAC into a set of attributes that are distributed by property specialists. Boolean formulas that define several get-to strategies are used to represent each set of characteristics.

For significant and permitted access, certain access methods are used. It eliminates the need to distribute components or create get-to-control lists for each device in the framework. According to the execution investigation presented in this work, the RSBAC conspiracy looks to provide a high degree of anonymity, resiliency, flexibility, and adaptability. Devices, ledger, chain code, and get to branch.

Specialist nodes are a part of the Consortium Blockchain Organize and are in charge of managing all the intuitive aspects of the Blockchain Organize for the benefit of the Consortium Blockchain Devices. When the requester submits an inquiry to the target, the target forwards it.

To verify the uniqueness of the requesters and the target's get to run the show, chain code is questioned by the enlisted get to accreditations are retrieved. After that, the permission get-to tree is constructed.

Blockchain is used to store final access data with the authorization outcome applied before outcomes are communicated to the requester.

based on property Managing three key-value stores, and the Get to right authority, allows for get to control.

When the Trait is enrolled, attribute title is granted to it, and person proprietor records are kept for each property, Suitable Access A completely pseudonymous approach without central administration is given in

Encourage clients to maintain control over their claim information. For the purpose of achieving pseudonymity, access control methods and Blockchain-like identifiers are used to identify all cooperation documents.

This control defined within the smart contract before being saved in Blockchain to provides insurance tokens for both sender and receiver of transaction which are used as an unique identification to verify the association's authorization for access to a specific asset.

To identify token limitation and reuse, exchange integrity checks and a two different discovery component are implemented. This suggested solution relieves the complexity of managing a significant block of induction control information based on prior works from the authorized consortium Blockchain devices. [26].

It might include a mix of administration nodes, operator nodes, smart contracts, Blockchain network, and chief nodes.

Chief Nodes,

II Compact nodes called supervisors have the responsibility to manage the access control rules.

Operator Node

iii A specific node is required to set up the smart contract on the Blockchain network, and that node will hold the smart contract during the duration of the get to control system.

Fourth: Smart Contract A piece of code that is sent in a Blockchain configuration may decide how each and every management-related operation will be carried out.

v. Blockchain management It uses a private Blockchain system to spare and handle admittance regulation policies.

vi. Administration center points.

For such approach, authors have optimized Blockchain for the capacity and distribution of access control data. All the activities recognized in the induction administrative framework are represented by a single clever contract that is both exclusive and unbreakable. The directors strike cunning deals to portray the structure's induction regulations.

The main advantage of this technique is its increased adaptability because other frameworks can be connected to the Blockchain setup simultaneously using special nodes called administration nodes.

A method for transferring data across geographically separated Consortium Blockchain devices was put forth by Hwang, D. et al. in [27].

Instead of sending a data request directly to the specific device, it is directed to the administration center, which then verifies for the access authorization stored in Blockchain. If the request is approved, the administration center accesses the information from that device and provides it to the inquiring device.

This approach is appropriate for far-flung devices where it is impossible to coordinate device communication. Additionally, for devices without listed get-to-control arrangements, dynamic approach generation is suggested.

As a result of this scheme, advanced versatility has been achieved Algorithm to resolve the security and protection concerns access control conspire with Blockchain execution which presented by Basudeb Bera [28].

It offers two different ways to gain control to start, is between two nearby rambles in the same flying range, in addition to inside the ramble and its Ground Station Server (GSS). GSS gathers the real-time information from the rambles and creates pieces using the exchanges. At that point, the cloud server receives these squares. Utilizing Convention Agreement Calculation, the pioneer cloud server among all cloud servers will confirm the item and add it to the Blockchain (RPCA).

Proposed conspire is ensured for “replay” and “man within the middle” assaults together as per the recreation reports. According to the recreation reports, a proposed conspiracy is guaranteed for "man in the middle" and "replay" attacks both.

Accordingly, public key cryptography can be used in many security layers, including entity authentication, and is necessary in every step of a consortium Blockchain to increase confidentiality. It is widely acknowledged that encryption and authentication are the two most crucial components of a Blockchain.

In order to use cryptography, both a private key and a public key must be present in a transaction.

To generate, revoke, manage, and store these generated keys in the consortium Blockchain's public key cryptography, they will need an authority.

Then, using ACL key management strategies that will be explained and compared, this methodology presents ways to improve Blockchain's privacy concerns.

By using the user's public key, any substance can confirm that a message is from a specific client. The message may also be partially encrypted sending it back at the moment. With its private key, that specific person can sign or decode the communication.

Various security objectives, such as material verification and confidentiality, can be performed with public key cryptography. The element authentication service can be provided through the signature/verification process, as shown in Figure. 4.

Everybody can verify or authenticate a content by approving the signature with the entity's public key on a message that is sent and tagged with its private key. Only the entity itself or someone with access to the private key can sign the communication because it is kept private. Ho ver, the confirmation is carried out using the open keys. Everyone who has access to the user's public information can confirm and validate their identity

Encryption and decryption, a similar process, can be used to provide the confidentiality service.

Using the recipient's public key, the sender encrypts the message.

The recipient uses his private key to do the decryption the receiver alone, or a person with the receiver's private key, will be able to read the data and decrypt it. Therefore, The security is ensured.

The user's ID, the generator's master private key, and the system parameter are all used to release the keys. The Identification and the public values are used by other hubs to generate a cypher text in order to encrypt a message.

To decipher the message, the client uses its own private key.

where the public key lacks a hierarchal identity and the signature is generated using the node's private key.

For instance, x@key1 rather than x is the public key of the X Organization Key 1.

The framework needs one PKG to create the secret key for the root, and the encryption phases in allowing a substance to generate private key an be driven from that key

Open key cryptography is a crucial security architecture that is widely utilized to provide the verification and confidentiality services.

For the majority of modern applications, including banking operations, such administrations are fundamental. A management framework is required to supply a proper infrastructure for such administrations.

section applies the RSBAC base to the next levels inside the ring phase.

Customer layer: The individuals or groups that require access to or storage of their data and services are included in the user layer.

• The management layer: Issuers, verifiers, and agreement nodes are part of the administrative layer. When the clients first arrive to execute their registrations, the issuers authenticate them.

Afterwards when, the verifiers certify the clients and look after their keys. The Blockchain's agreement hubs arrange and manage the unused squares similarly to how Bitcoin processing does

• The capacity layer:

In order to safely store and process the data, the capacity layer integrates virtualized data capacity and preparation In order to safely store and process the data, the capacity layer integrates virtualized data capacity and preparation In order to safely store and process the data, the capacity layer integrates virtualized data capacity and preparation foundations. To comply with the requirements for Banking records, the cube structure within the BBDS is modified by changing the exchange and piece header regions. Additionally, identity-based verification and encryption mechanisms are used to secure the system's intelligence. These methods are simple, reliable, and secure.

The transaction proceeds to the next step of decryption using the receiver's public key and private key if the ring test is successful.

pseudocode

```
  m sign message
  $R = \{K1, K2, ..., Kn\}$
$k\pi$ e private $K\pi \in R$.
Hn and Hp, hash functions.
RSBAC'Q'=1 verified else rejected
  1. Compute $K˜ = k\pi Hp(R)$
2. Create irrational values $\alpha \in R$ Zq and r ∈R
  Zq for $i \in \{0, 1, ..., n\}$ and i 6= $\pi$
  3. Calculate $c\pi+1 = Hn(R, K, ˜ m, \alpha G, \alpha K˜ )$
4. For $i = \pi + 1, \pi + 2, ..., n, 1, 2, ..., \pi - 1$ c,
  $n + 1 \rightarrow 1$ $ci+1 = Hn(R, K, ˜ m, riG + ciKi ,$
$riHp(R) + ciK˜ )$.
  5. $r\pi = \alpha - k\pi c\pi \pmod N$
  $\sigma(m) = (c1, r1, ..., rn, K˜ )$
-Signature confirmation
For $i = 1, 2, ..., n$
$n + 1 \rightarrow 1$ z `i = riG + ciKi z ``i = riHp(R) + ciK˜ c `i+1 =
Hn(R, K, ˜ m, zi `, zi `)Q==1
2. c`1 = c1
```

3.2 RSBACK group signature phase.

The present pseudocode bases uses this type of signature plot when exchanges have just one input. RSBAC is implemented using the following multi-output.

Using cryptography computations, clients have two sets of private/public keys (k1, K1) and (k2, K2). The privacy concept of functional segregation is made possible by using two sets of keys.

Private key k1 will be known as the "see key," while k2 will be the " commit key".

1. Receiver possesses both private and public keys (kB1 and kB2) (KB1, KB2). 1. The sender generates an irregular number r such that 1 r N and calculates the output public key to create one-time keys. Ko = Gn(rKB1) rKB1 + KB2.

2. Sender assigns a value rG to the exchange data and sends it to the arrangement, designating Ko as the payment's receiver.

Sender assigns a value rG to the exchange data and sends it to the arrangement, designating Ko as the payment's receiver. The recipient will use the respect rG to establish a shared secret comparable to Asymmetric cryptographic.

3. ave recognizes the data and recognizes rG. Thus, he is able to determine kB1 rG = rKB1. He will also be able to arrive to Ko = Hn(rKB1) G + KB2, as a result.

4. Ko = Hn make up the output's one-time keys (rKB1) G + kB2 G is equal to (Hn(rKB1) + kB2). G ko is equivalent to Hn(rKB1 + kB2).

He will be able to determine it is dedicated to him when he sees the yield's author.

The majority of transfers will have many outputs. In case nothing else, to exchange back any change to the sender himself. senders produce as it re irregular esteem r. The esteem rG is ordinarily known as the Transaction open key and is distributed within the Blockchain.

In transactions the same addressee is used more than once, the output file ensures that all output addresses are authentic and valid, each yield will have a list, and each incoming address will be different.

Sign Equation
$Ko = Hn(rKB1\ , l)G + kB2G = (Hn(rKB1\ , l) + kB2\ )G$ $ko = Hn(rKB1\ , l) + kB2$

Signature phase

The sender chooses q sets of estimate m, of extra irrelevant addresses from the consortium Blockchain, corresponding to clearly unspent yields. She blends the addresses in a Ring, including false commitments to zero that recognizing User-Misbehaviors in Group Signatures and Ring Signatures showing in Table 2.

The usual tracing	Level of User Privacy/ Traceability	Application Example
Normal tracing	▪ The normal tracing Suspected users are trackable ▪ Users that are innocent: traceable	▪ The key-card access architecture allows the group manager to keep track of user activities.
User dependent opening	▪ Users who would be suspected are trackable ▪ Users that are innocent	▪ When the buyer in an offer off refuses to pay, the master may reject any additional bids from that

	are untraceable	client without revealing the identification of the other respondents..
Decentralized tracing	▪ Users who are suspected are trackable ▪ Traceable for innocent users User anonymity is only secure from third parties.	▪ When a board member looks at a particular (ird) member's submitted article, he can identify him/her.
Message-dependent opening	▪ Traceable users suspected of sending messages ▪ Innocent users (not related to the message): non traceable	▪ Differentiating customers who entered a stop at a specific moment when an error occurred there.
Distributed tracing	▪ Users who are suspected are trackable ▪ Traceable for innocent users	▪ Shareholders agree about the need for a furious expert.

Accountable tracing	▪ Responsible tracing Users who are suspected are trackable ▪ Users that are innocent are untraceable	▪ Compliance ask the owner of a lodging facility to limit observation controls to a suspected list.
Accountable Ring signature scheme	Clients post in any online gatherings without enrolling, and users can only be tracked by their tracer.	▪ Gather Ring owner is able to identify a customer who violated the conduct code. Conduct code
Linkable Ring signatures	Ring signatures that can be linked User confidentiality is secure	▪ This prevents voting again during voting machines without recognizing use because only the link ability of signatures is determined.
Traceable Ring signatures	Digital certificates used by malicious users are tracked	▪ Outside of an assembly leader, an inert group can recognize confirmation, and a genuine customer can demonstrate their participation.

(Table 2. Tracking techniques for group signatures)

Even though there are certain research projects, providing an effective information protection advantage is still difficult. Effectiveness, adaptability, information ownership, and a lack of a defined information lifecycle approach are a few of the issues.

• Proficiency and Flexibility: Since the majority of information privacy approaches rely on intricate cryptographic calculations, scaling them to accommodate big applications is inefficient and difficult. Later research aims to make these cryptographic systems less complicated and more productive.

Whatever the case, the majority of the recommended alternatives still lack applicability.

Despite encouragement, most calculations are unable to keep up with the massive amount of information handling required by the existing networks.

Ownership and Control of Information: A fundamental aspect of protection is determining who is the owner of information and who has control over it. The party that selects the get-to-control rules for the information is, for the most part, the owner.

Unfortunately, the typical methods covered in the previous subsection still lack a resolution to the shareholding issue.

• Effective Information Lifecycle Approach: To effectively describe the lifecycle of the information, a framework for data protection needs to be created. This system should be able to identify the phases, describe their security requirements, and accommodate modifications to the lifecycle. These phases may involve the gathering, the distribution, and the termination of the knowledge and resources contained in the framework.

However, most people are still unaware of the value of a systematic privacy techniques.

Right Access has been used to provide a distributed, secure, and adaptable ACL administration.

The idea behind the proposal is to enable clients to register their modern assets and define their access agreements using the smart contracts connected to those assets. There are various steps involved in the asset request process.

Request for an asset held by client A is coordinated to the Blockchain network when it is made. The Blockchain organization then decides whether to grant or deny the request based on the clever contract for the relevant resource. The requester receives a response from the organization confirming or rejecting his access request. By implementing deep reinforcement learning, a flexible machine learning component, the owner can modify his or her access policy in light of feedback received from the Blockchain network.

The approaches review in the previous paragraph face a number of difficulties, such as inefficiency, complexity, a lack of security, and centralized controllers with a few levels of interoperability, which render the logging strategies ineffective. In order to change the supply stack and ensure adaptability, cloud resources may shift, making it difficult to follow assets. A further level of complexity can be added to the framework by using sophisticated security techniques like enhanced signature and encryption. However, in the event that the source and ownership of the data are made known to a third party, the lack of encryption and signature could compromise the security of the material. Finally, a centralized controller is necessary to store the logging data or to screen the data in a framework, which needs a trusted third party that's complex and a single point of disappointment.

4. CONCLUSION

The proposed approach help covering the common barriers of public Blockchain it can give the information ownership solutions and powerfully alter the get to rights when needed. Be that as it may, since the Blockchains depend on cryptographic strategies, the Blockchain-based strategies are still complex. The issues related with the traditional approaches and how the Blockchain innovation can unravel them.

A framework for the data security ought to be built to efficiently define the lifecycle of the information. This system ought to distinguish the phases, characterize their privacy prerequisites, and allow flexibility within the lifecycle changes. These stages can include the securing, the sharing and the erasure of the information and the assets included within the framework.

Be that as it may, a systematic approach is still lost in most of the proposed privacy techniques.

By restrain services cost is and time that the transaction diminishes it by expanding number of trusted get to list of mineworkers /banks/ controls without change or changes in organization structure, handle, procedure, or culture. Consortium Blockchain will give ensure of the Proprietor for successes transaction and secure data and programmer can't adjust and broadcasting an exchange once more which can break the transaction confirmation.

The proposed approach supports workflow and non-workflow systems. The proposed approach has an active security model, which means that it has active runtime management of tasks progression to completion and permissions assigned to tasks.

investigated the major flaws in Blockchain and proposed some possible solutions. These advantageous features and This ongoing development make new electronic cash system concept a serious rival to Blockchain, outclassing all its forks. proves that the existence of concurrent independent currencies has a huge positive effect. Each currency issuer (or developer in This case) is trying to attract users by improving his product. Currency is like a commodity: it can have unique benefits and shortcomings and the most convenient and trusted currency has the greatest demand.

The biggest support as an open source project would come from its own users, who are interested in it. consider as a full replacement to Blockchain. On the contrary, having two (or more) strong and convenient currencies is better than having just one. Running two and more different projects in parallel is the natural flow of electronic cash economics.

In this thesis, a new database access control model is presented as an extension to CPBAC model and PBFW model. The newly proposed approach is based on the characteristics of roles, purposes, tasks and policies

The proposed approach has present alternative solution for Barriers of Blockchain Barriers by the following features:

- Distributed Access Management.
- more Information extracted conditionally assuring the same user privacy.
- dynamic and Active permission assignment.
- authorization policies to support dynamic separation of duty.
- permission inheritance scope, eliminating the shortage of high management complexity.
- caused by inherited relationship in the traditional model that will save time.
- suitable for workflow and non-workflow systems.

5. FUTURE WORK

1. Study possibilities of the improving proposed approach to be extended approach for Hyper ledger Projects.

2. Study possibilities of the proposed approach to be extended over distributed systems or other Blockchain platforms through hard frogs.
3. Study possibilities of the proposed approach to be extended over Blockchains environments. Also, during implementation the following extensions re discovered to be useful.
4. De-centralized management of permission assignment.
5. There will be many policies in enterprise environment, and as a result it is important to manage authorization policies and optimize policy description.

REFERENCES

[1] Sam Mire. Blockchain-use-cases-banking. Published at [Online]

[2] Archana JoshiA.survey on security and privacy issues of Blockchain technology.

[3] Blockchain Council, Blockchain Ecosystem. Published at [Online]

[4] Adam Bender, Jonathan Katz, Ruggero Morsell. Ring Signatures: Stronger De_nitions, and Constructions without Random Oracles.

[5] Tara Salman, , Maede Zolanvari, Aiman Erbad, RajJain, Mohammed Samaka. Security Services Using Blockchains: A State of the Art Survey

[6] Dubai 2018 Fintech Conference . " Blockchain's Implications on FinTech Ecosystem & Innovation "

[7] Fran CasinoThomas K. Dasaklis Constantinos PatsakisNakamoto. literature review of Blockchain-based applications: Current status, classification and open issues.

[8] Thomas kitsantas1 , Athanasios Vazakidis and Evangelos Chytis . Review of Blockchain Technology and Its Applications in the Business Environment.

[9] Shang GAO, Tianyu ZHENG, Yu GUO , Bin XIAO. Efficient and Post-Quantum Zero-Knowledge Proofs for Blockchain Confidential Transaction Protocols.

[10] Chia-Chen Lin, Chin-Chen Chang, Yao-Zhu Zheng 3. A Ring Signature Based Anonymity Authentication Scheme for Group Medical Consultation.

[11] Rubdos. Entity Ring signature, Published at [Online]

[12] O. Kurbatov, P. Kravchenko,,T. Kuznetsova . Using Ring Signatures For An Anonymous E-Voting System.

[13] Pierangela Samarati1, Sabrina De Capitani di Vimercati. Access Control, Policies, Models, and Mechanisms, lecture notes In Computer Science.

[14] Sunoo Park Adam Sealfon Reputability . .Unclaimability of Ring Signatures.

[15] E. Bresson, J. Stern, and M. Szydlo. Threshold Ring signatures and applications to ad-hocgroups.

[16] N. Li, M. V. Tripunitara .On safety in discretionary access control, IEEE Security and Privacy.

[17] National Institute of Standards and Technology NIST SP 800-95. under Policy Based Access Control (PBAC) Published at [Online]

[18] Gang Ma, Kehe Wu, Tong Zhang, , Li. A. FlexiblePolicy-Based Access Control Model for Workflow Management Systems.

[19] Jing-Mei Li, Bin Wang, Nan Ding, Shengnan Jin. Access Control Model Based on Multi-Role and Task.

[20] Rana Elgendy, Amr Morad , Hicham G. Elmongui, Ayman Khalafallah, Mohamed S. Abougabal. Role-task conditional-purpose policy model for privacy preserving data publishing.

[21] Rebekah Mercer. Privacy on the Blockchain: Unique Ring Signatures.

[22] Secure Hash Standard. National Institute of Standards and Technology NIST 180-2. Published at [Online]

[23] Gavin Wood. Ethereum. A Secure Decentralized Generalized Transaction Ledger – Homestead Revision.

[24] hristopher Natoli, Jiangshan Yu∗ , Vincent Gramoli , and Paulo Esteves-Verissimo. Deconstructing Blockchains.

[25] Guy Zyskind, Oz Nathan, Alex Pentland. Enigma. Decentralized Computation Platform with Guaranteed Privacy.

doi:10.20944/preprints202209.0413.v1

[26] Ouaddah, A., Abou Elkalam, A., Ait Ouahma. A new Blockchain-based access control framework for the internet of things. Security and Communication Networks.

[27] Li, K., Lau, W. F., Au, M. H., et al. Efficient message authentication with revocation transparency using Blockchain for vehicular networks.

[28] Bera, B., Chatterj, D., & Das, A. K. Designing secure Blockchain-based access control scheme in IoT-enabled Internet of Drones deployment.

[29] Satoshi Nakamoto. Blockchain. A Peer-to-Peer Electronic Cash System.

[30] Chaum, D.; Van Heyst, E. Group signatures. In Workshop on the Theory and Application of of Cryptographic Techniques.

[31] Rivest, R.L.; Shamir, A.; Tauman, Y. How to leak a private In Proceedings of the International Conference on the Theory.

[32] Kurt M. Alonso , Jordi Herrera Joancomart´ı Monero Privacy in the Blockchain.

[33] Nicolas van Saberhagen. Cryptonote.