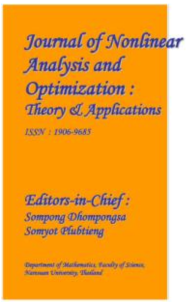

Journal of Nonlinear Analysis and Optimization : Theory & Applications
ISSN : 1906-9685
Editors-in-Chief :
Sompong Dhompongsa
Somyot Plubtieng
Department of Mathematics, Faculty of Science, Naresuan University, Thailand

Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1: 2025
ISSN : **1906-9685**

A PRIMORDIAL DIGITAL SIGNATURE AND ITS SIGNIFICANCE IN BLOCKCHAIN

NUKANABOINA LAKSHMIDEVI, PG SCHOLAR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, SREEDATTHA INSTITUTE OF ENGINEERING AND SCIENCE SHEERIGUDA, IBRAHIMPATNAM HYDERABAD, TELANGANA, INDIA.
Dr. NAZIMUNISA, ASSISTANT PROFESSOR(Ph.D.), DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, SREE DATTHA INSTITUTE OF ENGINEERING AND SCIENCE, SHERIGUDA IBRAHIMPATNAM HYDERABAD TELANGANA, INDIA.

Abstract: Digital signatures are essential for verifying the validity and integrity of electronic documents and transactions. With the advancement of blockchain technology, the need for safe digital signatures has increased. The article introduces and elucidates the "Prehistoric Trademark," a unique digital trademark system, using Blockchain as an illustrative case.
In primordial essence, the concepts of encryption and prime numbers intersect. Utilising the fundamental properties of prime numbers, it generates distinctive signatures that are resilient to diverse cryptographic attacks. The method employs a sequence of prime number operations to produce signatures that are secure and computationally efficient.

Within the framework of blockchain technology, Primaeval Trademark offers several benefits. Its principal role is to protect blockchain transactions against prevalent cryptographic assaults and ensure their authenticity. Secondly, its rapid processing facilitates expedited transaction management in blockchain settings with constrained resources. The third characteristic of Primaeval Signature is its scalability, enabling blockchain networks to accommodate an increased volume of transactions without compromising security.

This paper offers a thorough evaluation of the primal signature formula, including its computational efficiency, mathematical principles, and security robustness. Primitive trademarks on blockchains are examined, including their implementation details and their comparison to other digital trademark systems.

Key words: Blockchain, digital signature, privacy protection.

INTRODUCTION

Electronic trademarks are essential for the integrity and protection of electronic data and transactions. Their importance is in their provision of safe internet connections and transactions. The need for resilient digital trademark algorithms has intensified because to the emergence of blockchain technology, which utilises encryption to facilitate decentralised and secure transactions.

Our "Primaeval Trademark" formula is a novel approach to digital trademarks, and we discuss its potential to revolutionise blockchain innovation. Digital trademarks developed by Primaeval Signature are both efficient and safe, since they use the intrinsic residential or commercial properties of prime numbers. Primaeval Trademark presents a unique methodology in cryptography by integrating prime number theory to provide a reliable and secure trademark system. Prime numbers have always been used in encryption, although this application is unique. Primaeval Signature offers a novel viewpoint on electronic signature algorithms by using the intrinsic characteristics of prime numbers.
This article will examine the fundamental mathematical principles of trademarks and demonstrate how the concept of prime numbers offers a safeguard. We will highlight the algorithm's effectiveness and robustness against prevalent cryptographic attacks as we examine its fundamental components and techniques. Furthermore, we shall examine Primaeval Signature and its correlation with Blockchain Modern. The blockchain, a distributed journal innovation using cryptographic methods, guarantees the security of transactions and the ongoing organisation of all network participants. Electronic trademarks

are essential in Blockchain networks for authenticating transaction legality. Thus, the digital trademark algorithm selection directly influences the performance and security of the blockchain system.

Primaeval Signature provides unique benefits concerning blockchain applications. The blockchain's comprehensive security protocols render it impervious to cryptographic assaults. Due to its computational efficiency, it operates under low-power settings, enabling expedited transaction processing and broader blockchain network coverage. This brief article will examine the possible implications for scalability, performance, and security associated with the use of primordial trademarks in blockchain networks. By comparing Primaeval Signature with current digital signature methodologies used in blockchain technology, we may identify avenues for enhancement and demonstrate its advantages. Primitive Trademark is an innovative paradigm in digital trademarks that has the potential to transform blockchain functionality. This work uniquely integrates cryptography with prime number theory, illustrating the role of digital signature algorithms within the burgeoning blockchain business.

RELATED WORK

Contemporary digital trademark solutions are essential for ensuring the security and validity of blockchain transactions. Among all blockchain algorithms, the ECDSA is the most widely used digital signature algorithm. The first presentation of ECDSA, a technique for producing and authenticating digital signatures using elliptic curve cryptography, was conducted by the National Institute of Standards and Technology (NIST). Each user of the ECDSA system is assigned two cryptographic keys: a private key for transaction authorisation and a public key for signature verification. Deal launches are facilitated by clients' Personal Keys, and trademark verification may be conducted by other network members using the Sender's Public Key. This feature aims only to prohibit anybody other than the legitimate owner of the exclusive key from executing a transaction.

The Schnorr Signature is a prominent digital signature mechanism used by blockchain systems. Schnorr signatures provide many advantages to ECDSA, such as reduced signature size, enhanced security, and superior efficiency. Schnorr signatures enhance scalability and minimise transaction sizes by amalgamating several inputs into a single hallmark. Moreover, due to their resistance to certain cryptographic attacks, Schnorr Signatures provide an appealing alternative for blockchain applications. Although blockchain networks provide significant potential for selling Schnorr trademarks, roadblocks have arisen owing to compatibility challenges and the need for enhancements throughout the whole network.

The endorser may preserve their identity while engaging with others using Ring Signatures, a component of the Digital Trademark Privacy Enhancement Plan. Adi Shamir and Ron Rivest's Ring Signatures enable an individual to discreetly produce collective signatures. Ring signatures provide the capability to augment privacy and obscure the origins of Blockchain transactions. Ring Trademarks protects users' privacy and anonymity by making it very difficult to associate certain users with specific transactions when their signatures are aggregated. Despite their potential impact on blockchain scalability, the processing costs associated with Ring Signatures result in their infrequent use.

Two essential elements of blockchain technology are cryptographic hash functions and digital signature algorithms. Hash functions such as SHA-256 and SHA-3 guarantee the immutability and integrity of unique identifiers generated for transactions and blocks. These hash functions are essential to digital trademark systems since they provide a dependable method for hashing signatures and transaction data. The growing need for enhanced transaction processing efficiency and scalability blockchain networks has resulted in the creation of novel hash algorithms like BLAKE2. BLAKE2 is an optimal choice for blockchain applications where speed and efficiency are paramount, since it outperforms conventional hash algorithms.

Limit signature plans (TSS) are a domain of research aimed at enhancing and securing the digital signatures of blockchain networks. Various events may collaborate to create a Unified Trademark for a Message using TSS, hence distributing dependencies and reducing the likelihood of failure attributed to individual sources. Employing TSS in the framework of Blockchain Agreement Mechanisms facilitates the independent validation of Blocks, devoid of reliance on a single trusted entity, while safeguarding Transactions. Prior to the implementation of TSS on blockchain networks, it is crucial to thoroughly assess interoperability, scalability, and security issues.

Challenges with the Current Framework: Cryptographic methods such as ECDSA, Schnorr Signatures, and Ring Signatures—traditional forms of digital signatures—have seen extensive use in blockchain networks. However, some limits exist within these tactics that constrain their effectiveness and value. A significant concern with ECDSA is its vulnerability to being compromised by a quantum computer. Quantum computers may possess a considerable advantage over conventional computer systems in addressing certain mathematical problems, such as the discrete logarithm issue. The security of ECDSA may be undermined by advanced quantum computers, since it relies on the complexity of the Discrete Logarithm problem. This vulnerability casts doubt on the future of blockchain networks that rely on ECDSA for digital signatures.

Schnorr trademarks, similar to ECDSA, provide improved protection and smaller trademark sizes; nevertheless, their widespread adoption in blockchain networks has been hindered by compatibility issues. Evaluating existing blockchain protocols is essential for the integration of Schnorr signatures across various blockchain operating systems. Widespread promotion of Schnorr Signatures is challenging owing to the need of consensus on procedural changes while ensuring compatibility with existing systems.

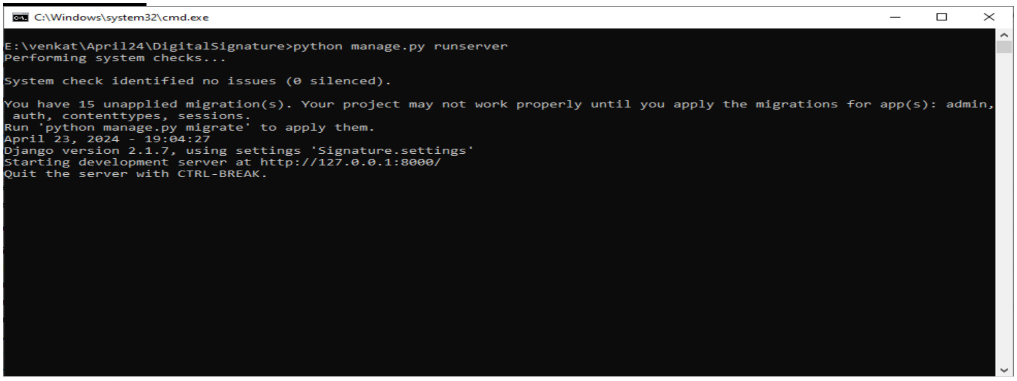
PROBLEM STATEMENT

Cryptographic algorithms such as ECDSA, Schnorr signatures, Ring signatures, and hash functions are essential for securing blockchain networks. However, these technologies face several significant challenges that limit their long-term viability. One major issue is that ECDSA, the most commonly used digital signature algorithm, is vulnerable to quantum computing. As quantum computers advance, they are expected to solve the discrete logarithm problem efficiently, which would undermine the security of blockchain systems that rely on ECDSA. Alternative cryptographic methods like Schnorr signatures offer enhanced security and scalability through smaller signature sizes and multi-signature schemes. However, their integration into existing blockchain networks has been slow due to compatibility challenges, requiring extensive modifications to current systems. This has prevented the widespread adoption of Schnorr signatures despite their potential advantages over ECDSA. Ring signatures, introduced to improve privacy, allow anonymous transaction signing within a group. However, their computational complexity grows with the group size, which impacts scalability and limits their effectiveness in high throughput blockchain environments .Cryptographic hash functions like SHA256 and SHA-3 play a critical role in ensuring data immutability and transaction integrity. However, these hash functions are not immune to collision attacks, and their computational expense can affect performance in blockchain applications with high transaction volumes. Although newer algorithms like BLAKE2 offer improved efficiency, they are still in the early stages of adoption. Threshold Signature Schemes (TSS) enhance security by distributing the signing process among multiple parties, increasing fault tolerance. However, interoperability and scalability challenges hinder the broad implementation of TSS in blockchain networks. Addressing these vulnerabilities and limitations is crucial for improving the security, efficiency, and scalability of future blockchain systems.

PROPOSED MODEL

The proposed model initiates with some **preprocessing of data**, followed by the elimination of unwanted words, symbols, and punctuation to make the text clean and structured. Properly formatted enhancement in a sentence and paragraph was also kept, which would improve the effectiveness of sentiment analysis and summarization. Then, **sentiment analysis** uses pretrained models to classify the polarity of each phrase or paragraph as positive, negative, or neutral. Sentiment analysis therefore applies more advanced techniques and more recent architectures, even deep learning models like transformer-based architectures that have been used in BERT or GPT, to achieve a high level of accuracy when detecting the sentiment classification. Following this are the **text summarization** steps, where an extraction and abstraction strategy is developed to create a summary. The method ensures that the summary ensures coverage of sentiment, is informative, and coherent. Sources are consolidated into a single summary that equilibrates all the significant elements. In the **sentimentdriven summarization** phase, the result of the sentiment analysis will be used to integrate into the process of summarization. Here, the phrases are selected based on their aspect of sentiment polarity so as to ensure that in the summarized version, the essence of the emotional tone of the original text is provided while ensuring that all the important emotional facets will be preserved. ROUGE would be used to evaluate the quality of summarization and sentiment-based text extraction. In addition to that, model accuracy, efficiency, and robustness are even evaluated with benchmark datasets. The optimization techniques such as parallel processing, caching, and version compression further improve the performance of the system. Hardware accelerators, like the use of GPUs, with distributed computing frameworks enhance the speed and scalability of the system. A **user interface (UI)** was designed to be accessible, taking inputs of text and displaying the generated summaries and sentiment analysis results. The UI is responsive, cross platform, and user-friendly, affording a straightforward experience. Deployment At completion, the system is deployed to a **production environment**, taking into account scalability, reliability, and security. Maintenance and monitoring processes were established to ensure smoothness of operation and constant improvement. Lastly, a **feedback loop** collects user feedback and monitors system performance to allow constant improvements in accuracy, usability, and efficiency. This ensures that the system adapts to meet the needs of users, with continuous improvement over time. This integrated model of summarization and sentiment analysis delivers high-quality output with optimally optimized performance at all times.

RESULTS

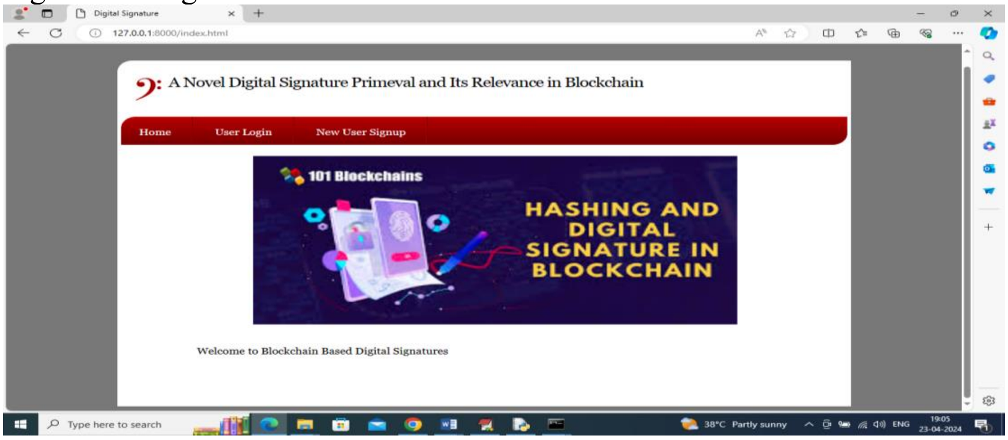


```
E:\venkat\April24\DigitalSignature>python manage.py runserver
Performing system checks...

System check identified no issues (0 silenced).

You have 15 unapplied migration(s). Your project may not work properly until you apply the migrations for app(s): admin,
 auth, contenttypes, sessions.
Run 'python manage.py migrate' to apply them.
April 23, 2024 - 19:04:27
Django version 2.1.7, using settings 'Signature.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CTRL-BREAK.
```

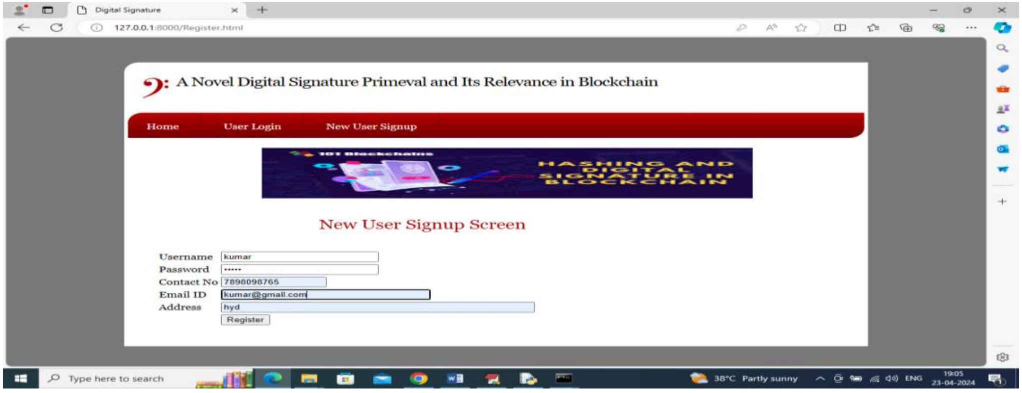
Fig 1: Running the Code



A Novel Digital Signature Primeval and Its Relevance in Blockchain

Welcome to Blockchain Based Digital Signatures

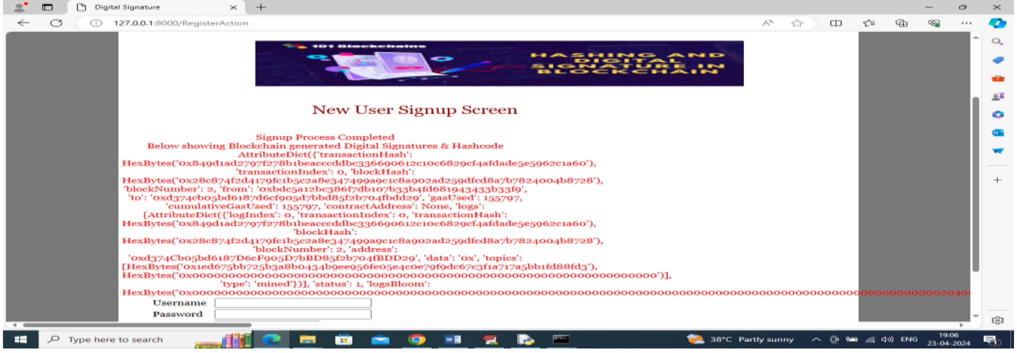
Fig 2: Homepage Screen


Digital Signature
127.0.0.1:8000/Register.html
A Novel Digital Signature Primeval and Its Relevance in Blockchain
Home
User Login
New User Signup
101 Blockchains
HASHING AND DIGITAL SIGNATURE IN BLOCKCHAIN
Type here to search
38°C Partly sunny
ENG
19:05
23-04-2024

New User Signup Screen

Username kumar
Password •••••
Contact No 7898098765
Email ID kumar@gmail.com
Address hyd
Register

Fig 3: Enter the Details

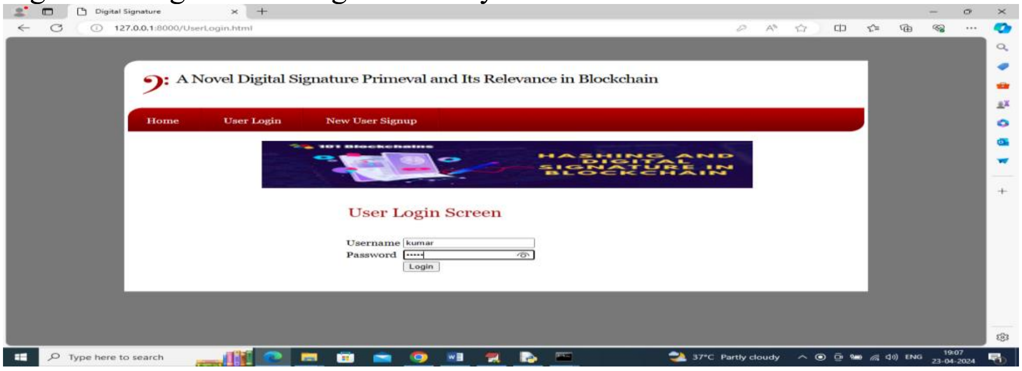


New User Signup Screen

```
                    Signup Process Completed
     Below showing Blockchain generated Digital Signatures & Hashcode
                  AttributeDict({'transactionHash':
HexBytes('0x849d1ad2797f278b1beacccddbc336690612c10c6829cf4afdade5e5962c1a60'),
                  'transactionIndex': 0, 'blockHash':
HexBytes('0x28c874f2d4179fc1b5c2a8e347499a9c1c8a902ad259dfcd8a7b7824004b8728'),
 'blockNumber': 2, 'from': '0xbdc5a12bc386f7db107b33b4fd681943433b33f9',
  'to': '0xd374cb05bd6187d6cf905d7bbd85f2b704fbdd29', 'gasUsed': 155797,
      'cumulativeGasUsed': 155797, 'contractAddress': None, 'logs':
   [AttributeDict({'logIndex': 0, 'transactionIndex': 0, 'transactionHash':
HexBytes('0x849d1ad2797f278b1beacccddbc336690612c10c6829cf4afdade5e5962c1a60'),
                            'blockHash':
HexBytes('0x28c874f2d4179fc1b5c2a8e347499a9c1c8a902ad259dfcd8a7b7824004b8728'),
                      'blockNumber': 2, 'address':
  '0xd374Cb05bd6187D6cF905D7bBD85f2b704fBDD29', 'data': '0x', 'topics':
[HexBytes('0x1ed675bb725b3a8b0434b9ee956fe05e4c0e79f9dc67c3f1a717a5bb1fd88fd3'),
HexBytes('0x0000000000000000000000000000000000000000000000000000000000000000')],
              'type': 'mined'})], 'status': 1, 'logsBloom':
HexBytes('0x000000000000000000000000000000000000000000000000000000000000000000000000000000000000002040
```

Username
Password

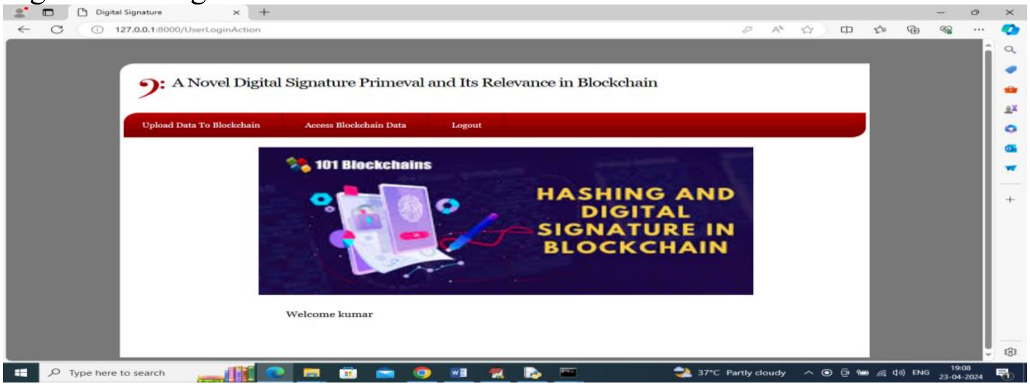
Fig 4: All Log Ddetails Ggenerated by Blockchain.


Digital Signature
127.0.0.1:8000/UserLogin.html
A Novel Digital Signature Primeval and Its Relevance in Blockchain
Home
User Login
New User Signup
101 Blockchains
HASHING AND DIGITAL SIGNATURE IN BLOCKCHAIN
Type here to search
37°C Partly cloudy
ENG
19:07
23-04-2024

User Login Screen

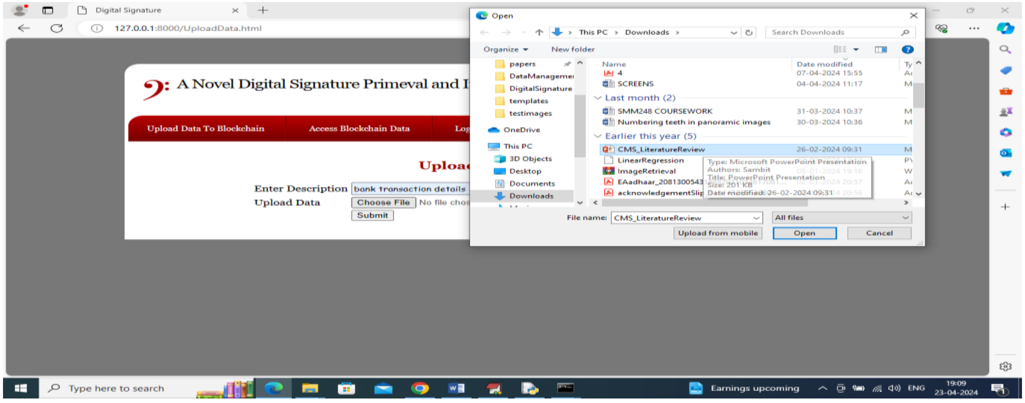
Username kumar
Password •••••
Login

Fig 5: User Login


Digital Signature
127.0.0.1:8000/UserLoginAction
A Novel Digital Signature Primeval and Its Relevance in Blockchain
Upload Data To Blockchain
Access Blockchain Data
Logout
101 Blockchains
HASHING AND DIGITAL SIGNATURE IN BLOCKCHAIN
Type here to search
37°C Partly cloudy
ENG
19:08
23-04-2024

Welcome kumar

Fig 6: Upload Data to Blockchain



Enter Description bank transaction details

Upload Data Choose File No file chos

Submit

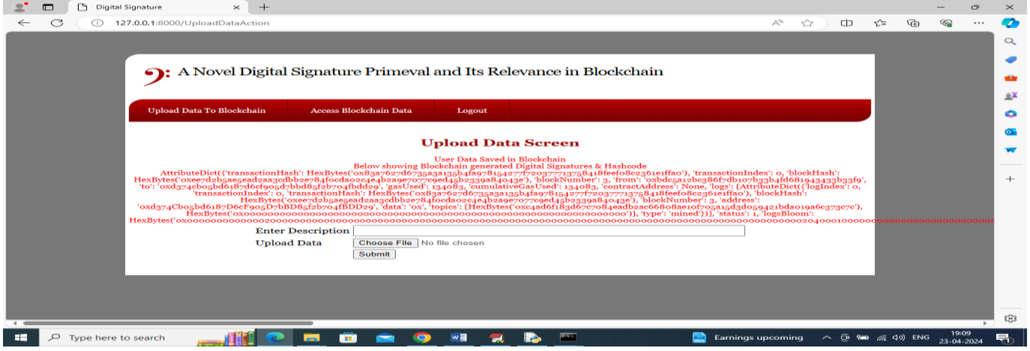
Name	Date modified
4	07-04-2024 15:55
SCREENS	04-04-2024 11:17
Last month (2)	
SMM248 COURSEWORK	31-03-2024 10:37
Numbering teeth in panoramic images	30-03-2024 10:36
Earlier this year (5)	
CMS_LiteratureReview	26-02-2024 09:31
LinearRegression	
ImageRetrieval	
EAadhaar_2081300543	
acknowledgementSlip	

Type: Microsoft PowerPoint Presentation
Authors: Sambit
Title: PowerPoint Presentation
Size: 201 KB
Date modified: 26-02-2024 09:31

File name: CMS_LiteratureReview

All files

Fig 7: Upload Desired File


Digital Signature
127.0.0.1:8000/UploadDataAction
A Novel Digital Signature Primeval and Its Relevance in Blockchain
Upload Data To Blockchain
Access Blockchain Data
Logout
Type here to search
Earnings upcoming
ENG
19:09
23-04-2024

Upload Data Screen

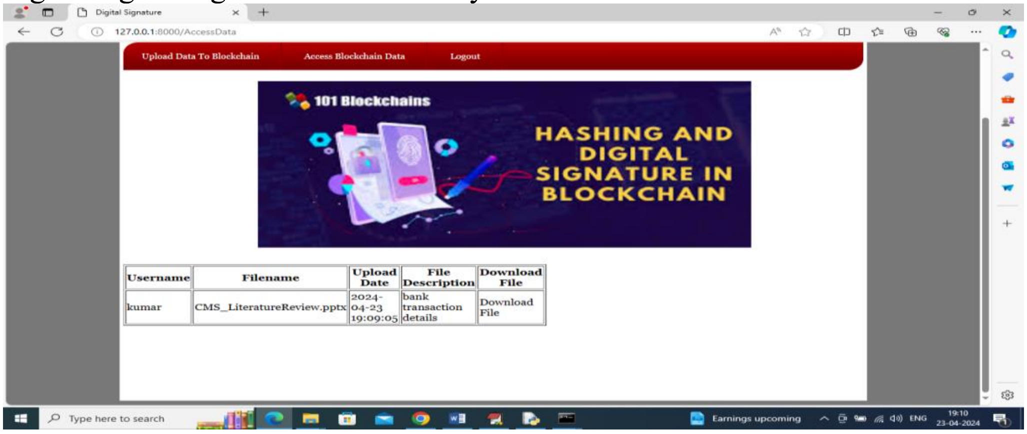
```
User Data Saved in Blockchain
Below showing Blockchain generated Digital Signatures & Hashcode
AttributeDict({'transactionHash': HexBytes('0x83a7627d6735a3a135b4fa978154277f720377713758418feef08c2361e1ffa0'), 'transactionIndex': 0, 'blockHash':
HexBytes('0xee7d2b5ae5ead2aa3cdbb2e784f0cda02c4e4b2a9e7077c9ed45b2339a84043e'), 'blockNumber': 3, 'from': '0xbdc5a12bc386f7db107b33b4fd681943433b33f9',
'to': '0xd374cb05bd6187d6cf905d7bbd85f2b704fbdd29', 'gasUsed': 134083, 'cumulativeGasUsed': 134083, 'contractAddress': None, 'logs': [AttributeDict({'logIndex': 0,
'transactionIndex': 0, 'transactionHash': HexBytes('0x83a7627d6735a3a135b4fa978154277f720377713758418feef08c2361e1ffa0'), 'blockHash':
HexBytes('0xee7d2b5ae5ead2aa3cdbb2e784f0cda02c4e4b2a9e7077c9ed45b2339a84043e'), 'blockNumber': 3, 'address':
'0xd374Cb05bd6187D6cF905D7bBD85f2b704fBDD29', 'data': '0x', 'topics': [HexBytes('0xc4ad6f183d67c7084eadb2ac66808ae10f705a15d3d059421bda019a6c373c7e'),
HexBytes('0x0000000000000000000000000000000000000000000000000000000000000000')], 'type': 'mined'})], 'status': 1, 'logsBloom':
HexBytes('0x00000000000000002000000000000000000000000000000000000000000000000000000000000000000000000000000204000100000000000000000000000000000
```

Enter Description

Upload Data Choose File No file chosen

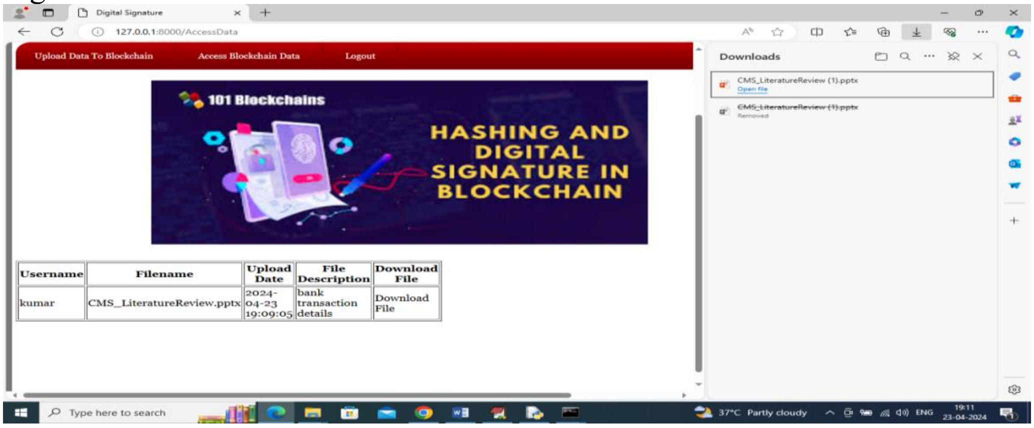
Submit

Fig 8: Digital Signature Generated by Blockchain



Username	Filename	Upload Date	File Description	Download File
kumar	CMS_LiteratureReview.pptx	2024-04-23 19:09:05	bank transaction details	Download File

Fig 9: Download File



CMS_LiteratureReview (1).pptx
Open file

~~CMS_LiteratureReview (1).pptx~~
Removed

Username	Filename	Upload Date	File Description	Download File
kumar	CMS_LiteratureReview.pptx	2024-04-23 19:09:05	bank transaction details	Download File

Fig 10: File Downloaded

CONCLUSION

The primitive signer is set to revolutionise digitally signed sophisticated technology and influence public blockchains. Its novel methodology, along with robust security, efficacy, and multi-threading capabilities, renders it a significant addition to the blockchain ecosystem. As blockchain evolves, primitive signer offers a safe and efficient basis for democratised trades, facilitating advancements and applications across many sectors. The primitive signer, an advanced digital signature technique, transforms blockchain systems and extensive medical technologies. Utilising its distinctive attributes, it offers a strong method for protecting transactions inside decentralised frameworks. In conclusion, the primordial logo is poised for a comprehensive digital redesign using new technology, while simultaneously playing a significant role in shaping public blockchains. Its unique approach, along with robust security, efficacy, and multithreading capabilities, as well as the ability to secure and safeguard displays, renders it a valuable addition to the blockchain technology ecosystem. Similar to the evolution of blockchain, primitive signer is strategically positioned to provide a secure and efficient foundation for democratised exchanges, aiming to open opportunities for growth while facilitating utilisation across diverse enterprises and applications.

FUTURE WORK:

One part of growth job includes additional research but also innovation complete help bolster the safety after all prehistoric signal group in particular information concerning. Whereas primordial signer deals rigorous tension of between computational chemistry hit, progression huge advances through evolutionary computation could necessarily entail even farther advancements to take care of it's own safeguards. Study in to other post-quantum cryptology as well as quantum-resistant optimization techniques can provide the new layers yeah safeguard group in particular future attacks.

REFERENCES

1. Adi Shamir and Ron Rivest. "Ring Signatures." Communications of the ACM, 45(10), 2002.

2. Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008.

3. Gregory Maxwell. "Schnorr Signatures: A Simple and Efficient Digital Signature Scheme for Blockchain." 2018.

4. Rosario Gennaro, Steven Goldfeder, and Arvind Narayanan. "Threshold Signature Schemes: Enhancing Security and Resilience in Blockchain Networks." IEEE Security & Privacy, 17(3), 2019.

5. Jean-Philippe Aumasson and Samuel Neves. "BLAKE2: Efficient Cryptographic Hash Function for Digital Signatures in Blockchain." International Workshop on Selected Areas in Cryptography, 2013.

6. Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps." Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2003.

7. Dan Boneh and Xavier Boyen. "Short Signatures Without Random Oracles and the SDH Assumption in Bilinear Groups." Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2004.

8. Jean-Sébastien Coron, David Naccache, and Mehdi Tibouchi. "Public Key Compression and Modulus Switching for Bilinear Maps." Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2013.

9. Allison Bishop, Ryan Henry, and David Pointcheval. "Non-interactive Zero-Knowledge Proofs for Composite Statements." International Conference on the Theory and Application of Cryptology and Information Security, 2003.

10. David Pointcheval and Olivier Sanders. "Short Randomizable Signatures." Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2016.