A Novel Method of Secure Child Adoption Using Blockchain Technology

Chetana Pujari, Chandrakala C B, Sharadruthi Reddy Muppidi, Sanjana Reddy Yalla and Manjula C Belavagi

Abstract—Child adoption is a noble procedure that establishes familial bonds between a child and prospective adopters (parents). However, the adoption process can be arduous due to various challenges. Prospective adoptive parents (PAPs) seek transparency and security to ensure a fair and unbiased outcome throughout this demanding process. The Central Adoption Resource Authority (CARA) and adoption agencies also emphasize the need for accurate information in prospective parent profiles. With the world transitioning into complete digitalization, traditional adoption procedures are becoming obsolete, warranting a shift towards more advanced methods. This paper proposes the implementation of blockchain technology to address the demands of a digitalized child adoption process, providing enhanced transparency and cybersecurity. Blockchain, with its secure and decentralized database, offers a promising solution. Our approach involves the utilization of smart contracts, privacy tokens, and decentralized data storage in blocks, connected through cryptography. These smart contracts are designed based on specific adoption policies, ensuring thorough verification of prospective adopters at the outset and maintaining transparency throughout the entire process. The adoption of blockchain technology holds significant potential to revolutionize and streamline the adoption process, offering a reliable, efficient, and secure platform for the formation of precious familial relationships.

Index Terms—Child Adoption, blockchain, smart contract, encryption, security.

I. INTRODUCTION

Blockchain technology and smart contracts have emerged as transformative solutions with the potential to revolutionize various industries, including child adoption. The primary objective of our application is to leverage blockchain technology, employing smart contracts to introduce transparency and security into the child adoption process [1] and [2]. Adoption, as a legal process, entails the transfer of parental rights from biological parents to adoptive parents while preserving genetic ties to the biological family.

II. BACKGROUND

A. Child Adoption Requirements

Child adoption in India falls under the purview of the Central Adoption Resource Authority (CARA), allowing Indian citizens, foreign nationals, and non-resident Indians (NRIs) to adopt, regardless of gender or marital status [3]. However, to be eligible for adoption, prospective adoptive parents (PAPs) must meet specific requirements, which are outlined as follows:

- Both PAPs are required to be financially, mentally, emotionally, and physically stable, without suffering from any life-endangering illnesses.
- The combined age of a couple seeking to adopt cannot exceed 110 years, and they must have completed at least two years of marriage, as well as reaching a joint consensus on the adoption.
- Couples with more than three children are generally ineligible to adopt, except in the case of special-needs children.
- For single parents, the maximum age for adoption is 55 years. Single females can adopt a child of any gender.
while single males can adopt any child, except for a girl.

- There must be an age gap of at least 25 years between the child and the parents, although this requirement does not apply to relative or step-parent adoptions. Similarly, specific criteria must be met for a child to be considered eligible for adoption, including:
  - Adoption is available for orphaned, deserted, or forfeited children who have been officially recognized as available for adoption by a child welfare committee.
  - A child without a legal parent or guardian, or whose parents are incapable of caring for them, is considered an orphan.
  - Children left alone or lacking parental or guardian care, and deemed abandoned by the child welfare committee, are categorized as abandoned.
  - Surrendered children, who have been declared by the child welfare committee due to uncontrollable physical, social, or emotional conditions by their parents, can also be considered for adoption.
  - To be eligible for adoption, a child needs to be declared "legally free."
  - If an abandoned child is found, the District Child Protection Unit publishes the child’s photograph and details in newspapers, and the local police are requested to trace the parents. Only after the police report stating that the parents are untraceable, the child is considered legally free for adoption.

These stringent requirements and considerations ensure that child adoption in India is conducted in a manner that prioritizes the welfare and well-being of both the prospective adoptive parents and the children in need of loving and stable families.

1) Child Adoption Process: The process of adopting a child in India is outlined below [4]. It begins with online registration on CARINGS (www.cara.nic.in), where prospective parents select an adoption agency and create a user ID and password. Valid contact details, including an email address and mobile phone number, are essential. Within 30 days of registration, parents must upload specific documents on the website. Failure to do so will necessitate re-registration. The required documents include:

- A photograph of the parent if single, or a family photo if married.
- Proof of residence, income, and one parent’s PAN card.
- Birth certificate, reason for adoption, and three letters of reference from individuals.
- Marriage certificate if married, divorce decree if divorced, or death certificate of the spouse if widowed.
- A certificate from a reputable medical practitioner confirming the absence of any diseases.

Following registration, the agency must be contacted, and original documents must be presented. Any inaccuracies can render the application invalid. The Special Adoption Agency (SAA) conducts a home study within 30 days of registration to assess the parents’ suitability for adoption. If deemed suitable, parents are placed on a waiting list, known as a "seniority list," where they can select one child from a preference of six children within two days.

After choosing a child, the parents can interact with the child and have a maximum of twenty days to make a final decision. Once the decision is made, documents are signed to formally accept the child. The SAA then files a petition in court, and adoptive parents sign it in the presence of a judge. Before finalizing the adoption, parents may take the child to pre-adoption foster care to better understand the child’s habits and needs.

During court sessions, the judge may inquire about the investment required for the child’s welfare. Adoption court orders are issued upon presenting the relevant receipt. Following the successful adoption, the agency is responsible for providing updates about the child’s well-being for two years in the post-adoption phase. This comprehensive process ensures the welfare of both the prospective parents and the adopted child throughout the adoption journey.

III. LITERATURE REVIEW

This section explores various aspects of the child adoption process, focusing on factors influencing international parents’ country selection for adoption [5], [6] and [7]. Prospective parents prioritize countries with low transactional costs, high adoption success rates, and shorter adoption processes [8]. However, the adoption system faces challenges related to excessive payments beyond the prescribed limit set by CARA [9]. Some parents are compelled to purchase life insurance policies or make donations and bribes, which make the process more expensive and raise concerns about transparency.

The COVID-19 pandemic has also impacted the adoption process negatively, resulting in longer waiting periods due to restrictions on in-person contact and court closures [10]. Amid the pandemic, there is a need for a more transparent adoption system with complete and accurate information about adoptive children [11]. Yet, some articles highlight the negative impacts of adoption on adoptive parents, such as the lack of medical records and genetic information about the child [12], [13] and [14].

The pandemic has led to the emergence of "COVID orphans," but adoption through social media requests raises concerns about child trafficking and illegal adoptions [15] [16]. The government’s efforts, like the Child Adoption Resource Information and Guidance System (CARINGS), have faced challenges and discrepancies, causing delays in the adoption process [17], [18]. Uncovering cases of illegal adoptions through NGOs highlights the desperation of prospective parents to avoid long waiting times [19].

Adoption laws in India are comprehensive but often lead to lengthy and strenuous proceedings for prospective parents, necessitating transparency and accuracy [20], [21] and [22]. Budget reductions can further impair adoption agencies’ work, while the lack of data and information poses challenges [23]. The time-consuming nature of the adoption process can discourage potential adoptive parents [24].

In conclusion, this literature review sheds light on the complexities, challenges, and ethical considerations involved in the child adoption process. Various factors, such as transparency, affordability, and access to information, play pivotal roles in shaping the adoption experience for both prospective parents and children. Addressing these issues is crucial for creating a more efficient, secure, and compassionate adoption system.
IV. BLOCKCHAIN

A. Need of Blockchain

The key features of blockchain technology address various challenges in different domains [25]. Here are some reasons why we need blockchain:

- Security - Data stored in a blockchain is of paramount importance and often contains sensitive information. Each new block of data is sequentially and chronologically linked with older blocks, forming a continuous chain of records. The blockchain’s end-to-end encryption ensures that the stored data remains tamper-proof and immutable. This inherent security feature prevents unauthorized activities or fraudulent alterations, enhancing the trustworthiness and integrity of the blockchain system.

- Transparency - Typically, organizations maintain separate databases, but blockchain operates differently by recording data in multiple locations using a distributed ledger or nodal structure. Each node possesses a copy of the blockchain, which is continuously updated with new blocks upon receiving confirmations. In the context of the Bitcoin blockchain, all transactions are openly accessible through personal nodes or blockchain explorers, enabling real-time visibility into any ongoing transactions. This transparency ensures that every Bitcoin’s journey can be traced regardless of its location, making the entire process traceable and accountable.

- Traceability - By leveraging blockchain technology, users can access accurate data about the provenance of products or information. Additionally, blockchain enables the detection of flaws or gaps in traceability, which can help identify and address issues that may cause delays in the respective processes.

- Smart contract - Automation within a blockchain application is facilitated through smart contracts, which are programmable scripts executed when specific conditions are met and recorded on the blockchain. These smart contracts are designed to automate the execution of agreements, ensuring immediate conclusions without the need for human involvement, intermediaries, or delays. The workflow is also automated, triggering the next step automatically once the predetermined conditions are satisfied, streamlining the entire process.

- Efficiency and Cost Savings - Traditional paper-based procedures have become outdated and inefficient due to their susceptibility to human errors and the need for frequent third-party interventions. In contrast, blockchain technology streamlines these processes, enabling faster and more efficient operations. Vital documentation and data can be recorded on the blockchain, eliminating the need for paper-based exchanges. Furthermore, the decentralized nature of blockchain removes the need to reconcile different ledgers, resulting in significantly more efficient clearing and settlement procedures with a reduction in associated costs.

B. Role of blockchain in child adoption process

Secure sharing of data between prospective adoptive parents (PAPs) and agencies is essential for building trust and facilitating adoption decisions, contract management, identity verification, and other services [26], [27]. Blockchain technology is particularly well-suited for the child adoption process due to the following reasons:

- Decentralization - Blockchain allows data to be distributed across multiple network nodes at different locations. This decentralized nature eliminates the need for intermediaries or middlemen, minimizing the risks associated with third-party interventions. Adoption records are securely stored and cross-referenced among nodes, making it extremely difficult to tamper with the information.

- Smart Contracts - Smart contracts are programmable codes embedded within the blockchain to facilitate, verify, or enforce contract agreements. In the context of child adoption, smart contracts can be tailored to adhere to the conditions and requirements set forth by the Central Adoption Resource Authority (CARA) or other relevant authorities [28]. These contracts automatically execute the agreed-upon terms when specific conditions are met, streamlining the adoption process.

For example, smart contracts can be designed to validate and verify documents provided by prospective adoptive parents (PAPs) against the criteria specified by CARA. Once the conditions are satisfied, the smart contract triggers subsequent actions, such as issuing notifications to PAPs or updating the blockchain with the relevant adoption information. Once recorded, the data on the blockchain is immutable, ensuring the integrity and privacy of the adoption process.

By leveraging the decentralized and transparent nature of blockchain technology, the child adoption process can become more efficient, secure, and trustworthy, benefiting both prospective adoptive parents and the agencies involved.

C. A brief explanation of smart contracts specific to the child adoption process

An aspiring adopter envisions adopting a child through a smart contract with an adoption agency. The agency commits to validating the adopter’s application promptly once their background aligns with the government’s stipulated requirements. Both the prospective adoptive parent (PAP) and the agency have distinct roles in the smart contract agreement, ensuring a smooth process that automatically exchanges the authentication letter or notification for digitally signed documents that meet the eligibility criteria on the agreed-upon date.

Should the agency fail to provide the authentication by the specified date, the smart contract promptly raises an alert, highlighting the issue. This innovative approach eliminates the need for any fees and the involvement of illegal middlemen, third-party intermediaries, or unauthorized adoption agencies.

By leveraging the power of smart contracts and blockchain technology, this streamlined adoption process enhances transparency, trust, and efficiency while safeguarding the interests of all parties involved.

V. PROPOSED MODEL

Our application utilizes the public, decentralized Ethereum blockchain, featuring smart contract functionality written in Solidity. Figure 1 illustrates the implementation of the child
adoption process through our Blockchain application. The key participants in this process are the prospective adoptive parents (PAPs) and the adoption agency.

The initial “signing up” process mandates PAPs to upload required documents as specified by the Central Adoption Resource Authority (CARA). Upon successful document uploading, the data undergoes processing through a hash function. For each document uploaded, a unique and random pattern of the same length is generated. This hash data ensures computational efficiency, regardless of the input data size.

A private key specific to each user’s transaction is then generated, accessible only to the respective user. Subsequently, the authentication of documents takes place when the user signs the hash of the document information [29]. This digital signature serves as authentication for the process. When the PAP submits their transaction, they must prove their authorization over the content to every other node in the peer-to-peer (P2P) network. The P2P network verifies and checks all other nodes to reach a consensus on authentication. The process is completed only when the corresponding public key is used for authentication.

Finally, the PAP receives an online acknowledgment, and their data is updated on the blockchain ledger in the form of a new data block [30]. These blocks are added to the blockchain ledger following the Ethereum protocol, generating the cryptocurrency Ether (ETH) in the process. The sequence diagram, as shown in Figure 2, provides a chronological representation of the entire adoption process, illustrating the interactions and messages involved. The diagram features prospective adoptive parents (PAPs) as the main actors and includes objects such as the website, web back-end, and adoption agency. The adoption process commences with the PAPs registering online on the website. Subsequently, the web back-end verifies the provided details and based on their authenticity, displays a message to the PAPs. If the credentials are valid, the PAPs receive an online acknowledgment; otherwise, a message indicating invalid details is shown.

Following the initial registration, the PAPs submit all the necessary documents as specified by the adoption agency. The web back-end then verifies the submitted documents using smart contracts. If the documents are found to be inaccurate, the website displays a message stating that the application is invalid for the PAPs. Conversely, if the submitted information is accurate, the website displays a message confirming the validity of the application.

Finally, the PAPs submit the original documents to the adoption agency, which then communicates the validation of the documents back to the prospective parents. The sequence diagram effectively illustrates the step-by-step flow of interactions in the adoption process. Figure 3 represents the blockchain database graph, showcasing the structure and relationships between nodes that form the database schema. On the other hand, Figure 4 displays the scrollable user interface (UI) page of the application. The UI starts with fields for entering name and email, where valid information must be provided. Following that, the marital status field presents four options: single, married, divorced, and widowed. Subsequent fields include a family photo, proof of residence, proof of income from the last year, birth certificate, one parent’s PAN card, marriage certificate or divorce decree, medical practitioner’s report, and three letters of recommendation, all requiring document uploads.

Table I lists the software tools used along with the versions used. The smart contracts are implemented using Solidity, an object-oriented programming language. These contracts were deployed using Remix IDE (Integrated Development Environment), as depicted in Figure 5. The execution of smart contract code occurs within the Ethereum Virtual Machine (EVM), where it is compiled into low-level bytecode by a Solidity compiler. During this stage, function calls and variable assignments are also debugged. To facilitate interaction with the Ethereum blockchain, Metamask, an Ethereum wallet, injects the web3.js JavaScript library into the user’s web browser. Metamask ensures privacy, security, and anonymity by not storing user data and allows seamless integration with various browsers of choice.

For smart contract deployment and testing, Ganache provides an in-memory blockchain that mimics an Ethereum node. It serves as an ideal environment to deploy and interact with smart contracts. By linking the RPC address of Ganache to Metamask and importing the corresponding private key, a new account is created and connected to Remix IDE. Once the smart contract is deployed on Remix IDE, gas or Ether (ETH) is utilized from Metamask to execute the transaction, resulting in a successful deployment. For document digital signatures, hashing is used to sign and verify the documents, as illustrated in the code snippet shown in Figure 6.

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node.js</td>
<td>v14.15.4</td>
</tr>
<tr>
<td>Solidity</td>
<td>v0.5.16</td>
</tr>
<tr>
<td>Ganache</td>
<td>v2.5.4</td>
</tr>
<tr>
<td>Metamask</td>
<td>v10.18.3</td>
</tr>
<tr>
<td>Remix IDE</td>
<td>v0.11.0</td>
</tr>
<tr>
<td>Web3</td>
<td>v1.3.5</td>
</tr>
<tr>
<td>Processor</td>
<td>Intel(R) Core(TM) i5-5200U CPU @ 2.20 GHz 2.19 GHz</td>
</tr>
<tr>
<td>RAM</td>
<td>16.0 GB</td>
</tr>
<tr>
<td>OS</td>
<td>Windows 10 Pro 21H2</td>
</tr>
</tbody>
</table>

Table II: Software Tools Description

<table>
<thead>
<tr>
<th>Software</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node.js</td>
<td>Real-time apps can be created using the open source Node.js (Node) server-side execution framework for JavaScript programming.</td>
</tr>
<tr>
<td>Solidity</td>
<td>For the purpose of building smart contracts on several blockchain systems, most notably Ethereum. Solidity is an object-oriented programming language which is used.</td>
</tr>
<tr>
<td>Ganache</td>
<td>A personal Ethereum blockchain is set up using Ganache to deploy contracts, develop applications, and run tests, giving the ability to perform all actions on the main chain without cost.</td>
</tr>
<tr>
<td>Metamask</td>
<td>Metamask is a web wallet that allows transactions for accessing Ethereum-based distributed applications, or Dapps.</td>
</tr>
<tr>
<td>Remix IDE</td>
<td>Remix IDE() is an open-source web application that facilitates the entire process of contract creation with Solidity and Ethereum.</td>
</tr>
</tbody>
</table>
VI. RESULTS

Our work addresses several inherent issues within the current adoption system, providing effective solutions. One of the major drawbacks was the lack of transparency, which has been overcome through our new system. The adoption agency’s proceedings and children’s data are constantly accessible to parents as they are stored on the Interplanetary File System (IPFS), ensuring complete transparency and minimizing malpractices. Both prospective adoptive parents (PAPs) and children benefit from the new system. PAPs’ information is saved on the decentralized blockchain, providing children with comprehensive knowledge about their potential parents, making the entire process credible and the verification process error-free. The use of smart contracts enables automated verification based on predetermined conditions, ensuring children find suitable parents through a faultless process. The digitization of the adoption process addresses the complexity and lengthy waiting periods that discourage PAPs from adopting. With digital document verification and automated processes, the entire adoption process becomes more efficient, taking around 2–3 months from registration to completion.

To address payment-related issues involving middlemen, our application requires a preliminary registration fee to be paid by PAPs during registration. All involved parties’ fees are recorded and predetermined in the code, preventing unauthorized charges and ensuring transparency. The new online adoption system provides adoption agencies with a suitable budget, and the transactional costs are as specified...
by the government, avoiding excessive fees. International adopters can view the costs and make informed decisions. During the COVID-19 pandemic, the adoption process faced challenges, leading to the abandonment of many "COVID orphans." Our application offers a potential solution by registering these children in the database, and efficiently connecting them with verified prospective parents seeking to adopt.

Overall, our work significantly improves the adoption process, enhancing transparency, efficiency, and the overall adoption experience for both parents and children.

A. Performance Analysis and Results

Figure 7 displays the graph illustrating the total gas usage per transaction (in ETH or Ethereum bucks), while Figure 8 represents the response time (in seconds) graph. Both graphs consist of 10 instances, each corresponding to a different testing scenario with unique inputs, varying numbers of entries in the blockchain ledger, and different numbers of nodes. Furthermore, Figure 9 visually portrays the sum of time taken for smart contract execution and digital signature verification. This graph provides insights into the combined processing time for these essential tasks. Lastly, Figure 10 exhibits distinct execution times for three different blockchain operations: add, update, and fetch records. Each value on the graph corresponds to a specific blockchain entry, enabling a comprehensive comparison of the execution times for various operations.

VII. SECURITY ANALYSIS

In this section, we highlight the security attacks that our proposed work can overcome. The following potential attacks have been mitigated by our solution:

1) Data Tampering: The use of blockchain technology ensures that the adoption records are tamper-resistant. Once data is added to the blockchain, it becomes immutable and cannot be altered, making it highly secure against data tampering attacks.

2) Unauthorized Access: Ethereum blockchain employs cryptographic keys for user authentication and access control. Smart contracts enforce permissions, allowing only authorized users (prospective adoptive parents, adoption agencies) to interact with the system, mitigating unauthorized access attempts.

3) Fraud and Misrepresentation: With the transparency and traceability of blockchain, it becomes difficult for malicious actors to engage in fraudulent activities or misrepresent information in the adoption process.

4) Middleman Interference: The use of smart contracts eliminates the need for middlemen or intermediaries in the adoption process.

5) Sybil Attacks: Ethereum blockchain’s Proof-of-Work (PoW) or Proof-of-Stake (PoS) consensus mechanisms make it difficult for attackers to perform Sybil attacks.


VIII. CONCLUSION

Our application aims to improve the child adoption process by addressing the complexities and lack of transparency that have hindered the journey for many prospective parents. In the adoption process, we ensure transparency and authenticity by using blockchains and smart contracts. Through
Fig. 4: User Interface (UI) - Home page

Fig. 5: Code snippet of Smart Contract

```java
contract Adoption {
    struct Adopter {
        uint id;
        string name;
        string mail;
        string marital;
        string desc;
    }
    mapping(uint => Adopter) public adopters;
    uint public count=0;
    constructor ()public {
        createAdopter();
    }
    event submittedEvent(
        uint indexed count
    );
    function createAdopter(string memory _name,
        string memory _mail, string memory _marital,
        string memory _desc) public {
        count++;
        adopters[count]=Adopter(count, _name, _mail, _marital, _desc);
        emit submittedEvent(count);
    }
}
```

Fig. 6: Code snippet of Hash algorithm used

```java
// Hash algo to find the signature
const hashAlgorithmId = forge.aes112.hmac256.hmacAlgorithm();
const hashAlgorithm = forge.pkcs8.pkcs8(hashAlgorithmId).toUpperCase();

// Verifier creation
const buf = Buffer.from(forge.asn1.toDerSet().data, "binary");
const verifier = crypto.createVerify("SHA-1" + hashAlgorithm);
verifier.update(buf);

// Verification
const cert = forge.pkcs8.certificates[0] instanceof forge.certificate;
const validAuthenticatedAttributes = verifier.verify(cert, sig, "binary");
if (!validAuthenticatedAttributes) throw Error("Wrong authenticated attributes");

// Creation of hash of non-signature part of EDF
const pdfHash = crypto.createHash(hashAlgorithm);
const data = extractedData.signature;
pdfHash.update(data);

// Extraction of the message digest
const oid = forge.pkcs8.oids;
const fullAttrDigest = attrs.find(
    attr => forge.asn1.dereference.value(0).value() == oid.messageDigest
);
const attrDigest = fullAttrDigest.value(1).value(0);
```
blockchain-based smart contracts, we provide adopters with a clear view of the eligibility criteria, making it easier for them to fulfill the requirements. As part of the security protocol, the adopter’s data is encrypted and safeguarded, ensuring their privacy and security. Furthermore, smart contracts automate the authentication of submitted documents, reducing delays and streamlining the verification process. Overall, our application successfully gets around the challenges that are now present, streamlining the adoption process and matching prospective parents with kids who need a loving home. We work to make the adoption process satisfying and beneficial for all parties by attaining transparency, security, and authentication.

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CARA</td>
<td>Central Adoption Resource Authority</td>
</tr>
<tr>
<td>2</td>
<td>PAP</td>
<td>Prospective Adoptive Parent</td>
</tr>
<tr>
<td>3</td>
<td>CAS</td>
<td>Child Adoption System</td>
</tr>
<tr>
<td>4</td>
<td>NRI</td>
<td>Non Resident Indian</td>
</tr>
<tr>
<td>5</td>
<td>DCPU</td>
<td>District Child Protection Unit</td>
</tr>
<tr>
<td>6</td>
<td>SAA</td>
<td>Special Adoption Agency</td>
</tr>
<tr>
<td>7</td>
<td>CARINGS</td>
<td>Child Adoption Resource Information and Guidance System</td>
</tr>
<tr>
<td>8</td>
<td>NGO</td>
<td>Non-Governmental Organization</td>
</tr>
<tr>
<td>9</td>
<td>IDE</td>
<td>Integrated Development Environment</td>
</tr>
<tr>
<td>10</td>
<td>EVM</td>
<td>Ethereum Virtual Machine</td>
</tr>
<tr>
<td>11</td>
<td>RPC</td>
<td>Remote Procedure Call</td>
</tr>
<tr>
<td>12</td>
<td>ETH</td>
<td>Ether</td>
</tr>
<tr>
<td>13</td>
<td>IPFS</td>
<td>InterPlanetary File System</td>
</tr>
</tbody>
</table>

REFERENCES