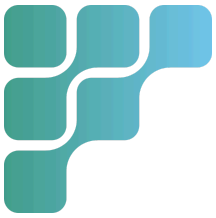

The Foreground Network

Abstract

This whitepaper proposes a novel approach to conducting background checks using a dedicated blockchain network and peripheral artificial intelligence. This system aims to bring the background check process into the foreground, enhancing requester transparency, maintaining candidate privacy, reducing fraud, and streamlining the verification process. The proposed model introduces a permissioned blockchain where users control access to their data through temporary keys, and employers can request background checks with assured authenticity and compliance.

Scott Bratcher, Mark Lingo, and William Gill

V.1.0 Last updated December 15, 2024

"In twenty years, not one piece of ingenuity has been applied to the researcher side. Not one."

- Mark Lingo, Brango Software Solutions

Introduction

Background checks are essential for employers to verify the credentials and history of potential employees. Traditional methods are often time-consuming, susceptible to fraud, and pose significant privacy concerns. With the advent of blockchain technology, there is an opportunity to revolutionize this process by creating a secure, transparent, and efficient system.

This whitepaper outlines a blockchain-based solution for background checks, detailing the mechanisms for requesting background checks, data onboarding, privacy preservation, and incentive/penalty systems.

Contents

Definitions

Applicant / Candidate

An individual who may have applied for a position or opportunity and is subject to a *background check*. The terms "*Applicant*" and "*Candidate*" are used interchangeably to refer to the person whose background information is being verified.

Background Check

A process of verifying an individual's personal, educational, employment, and criminal history.

Contestation Mechanism

A structured process that allows parties (*employers* and *candidates*) to dispute the contents of a *background check* report if inaccuracies or discrepancies are found. It involves submitting a dispute to the network for resolution.

Data Access Permissions

Authorizations granted to specific parties (*employers*, *researchers*) to access certain data within the system. Permissions are controlled through cryptographic keys and smart contracts.

Dispute Resolution

The process of addressing and resolving disputes submitted through the *contestation mechanism*. It involves reviewing evidence, evaluating claims, and making a decision to correct or uphold the *background check* report.

Employer / Requester

An organization or person(s) seeking to verify the background of a *candidate*. The terms "*Employer*" and "*Requester*" are used interchangeably to refer to the entity initiating the *background check* request.

Node

A participant in the blockchain network that maintains a copy of the ledger and contributes to transaction validation. Nodes can represent *employers*, *candidates*, *researchers*, or other entities in the network.

Researcher / Researcher Node

A trusted and authorized entity within the network responsible for conducting *background checks* when *candidates* do not respond to requests. Researchers have access to necessary data and are bound by confidentiality agreements.

Response Window

The designated time period (proposed 24 hours) within which a *candidate* must respond to a *background check* request. If no response is received, the *no-response* protocol is initiated.

Smart Contract

A self-executing contract with the terms of the agreement directly written into code on the blockchain. Smart contracts automate processes such as granting access permissions, enforcing rules, and handling transactions.

Temporary Access Key

A cryptographic key generated by a *candidate* or the system to grant limited-time access to encrypted background information. It ensures that only authorized parties can access the data for a specified duration.

Token

A digital asset used within the blockchain network to incentivize participation and honest behavior. Tokens can represent rewards for candidates or be used to enforce penalties.

Fungible Token: Tokens that are interchangeable and have equal value, similar to currency.

Non-Fungible Token (NFT): Unique tokens representing specific assets or credentials, not interchangeable with other tokens.

Transaction

A recorded operation on the blockchain that represents actions such as background check requests, candidate responses, or data access grants. Transactions are validated and stored in blocks.

User

A general term referring to any participant in the system, including employers, candidates, researchers, and other entities interacting with the blockchain network.

Verification

The process of confirming the accuracy and authenticity of information provided by *candidates*. Verification is conducted by *employers*, *researchers*, or automated systems within the network.

Network Architecture Overview

The Foreground Network is a dynamically reflexive **Proof-of-Authority** permissioned network designed specifically for background checks. It leverages smart contracts to automate processes, ensure data integrity, and manage permissions.

A novel blockchain network where:

Employers can request background checks with a 24-hour notice.

Candidates can respond to these requests, confirming their identity and granting access to their data.

Researchers step in if candidates do not respond within the notice period.

Token Incentives reward participants for their engagement.

Key foundational requirements:

Decentralized Network: Nodes representing requesters, candidates, and researchers.

Custom Blockchain: A tailored blockchain specifically for conducting background checks.

Security Measures: Encryption, hashing, and temporary access keys.

Background Check Process Overview

Step 1: Employer Initiates Background Check

When an employer or requester wants to conduct a background check, they submit a request to the blockchain network containing a hash of the candidate's full legal name and birthdate.

Step 2: Matching Candidates Are Notified

The network searches for users whose hashed personal information matches the hashed candidate information provided by the employer. Notifications are dispatched to these users and candidate nodes monitor the blockchain for transactions matching their info hash.

Step 3: Candidates Respond to Notice

Candidates who recognize the request can respond by confirming their identity. This grants the employer temporary access to their encrypted background information.

Step 4: No Response Protocol

If no candidates respond within 24 hours, a designated researcher node is authorized to access the necessary data to compile the background check.

Step 5: Researcher Compiles and Delivers Results

The researcher accesses the necessary data using their permissions and compiles the background check report. The results are then delivered to both the employer and the candidate, with options for contestation.

Step 6: Contestation Mechanism

Both the employer and the candidate have the option to contest the report if inaccuracies are found. They can submit a dispute to the network for resolution.

Background Check Process Detailed

Step 1: Employer Initiates Background Check

In this section, we delve into the first step of the blockchain-based background check system: how an employer or a general requester initiates a background check by submitting a request to the blockchain network.

Data Preparation

The employer collects the candidate's full legal name and birthdate. The employer should have received consent from the candidate to perform the background check.

Hashing Personal Information

The employer hashes this information to create a unique identifier without exposing sensitive data. Hashing converts the input data into a fixed-size string of characters, which is irreversible, ensuring that the original data cannot be retrieved from the hash.

Creating the Request Transaction

The employer creates a transaction that includes the hashed candidate information and other relevant details. The transaction is added to the pending transactions pool and will be sent to a requester node.

I. From Address: Requester's blockchain address.
II. Type: Identifies the transaction as a background check request.
III. Candidate Hash: The hashed candidate information.
IV. Timestamp: Current time in epoch milliseconds.
V. Notice Expiry: The deadline for the candidate to respond (e.g., 24 hours from the timestamp).

Step 2: Matching Candidates Are Notified

This process ensures that only the relevant candidates are alerted while maintaining the privacy and security of personal data. Candidates may actively monitor the blockchain for transactions matching their information hash, enabling them to respond promptly to background check requests. Candidates may either set up their own candidate node or opt-in to an existing node via email alerts or their preferred method of communication.

Hash Matching

The network searches for users whose hashed personal information matches the hash submitted by the employer. Candidates who are part of the network have previously registered their hashed personal information on the blockchain during the onboarding process. Each candidate's hashed data is associated with their blockchain address and public key, which are used for communication and verification purposes.

Candidate Monitoring

Candidates monitor the blockchain for transactions containing hashes that correspond to their own. When a new background check request is added to the blockchain, nodes scan the stored hashed personal information of registered candidates to find matches with the employer's submitted hash.

Notification Dispatch

Once a match is found, notifications are sent to the relevant candidates. The candidate's client software can automatically generate an alert or notification for the candidate to take further action. This will be executed on-chain and may also be followed up off-chain, utilizing channels such as email, SMS, or push notifications, with references to the on-chain transaction.

Privacy Preservation: The process is designed to protect personal data by using cryptographic hashes instead of raw information. Since only hashes are compared, the actual personal information is never exposed or transmitted.

Step 3: Candidates Respond to Notice

The process is designed to ensure that candidates have control over their personal information while maintaining the integrity and reliability of the background check system. Importantly, candidates are rewarded for accurate and timely participation, and they may be penalized for inaccuracies or fraudulent responses. This incentivizes honesty and engagement, enhancing the overall effectiveness of the system.

Key Components:

I. Candidate Verification and Consent
II. Granting Temporary Access
III. Reward Mechanism for Accurate Participation
IV. Penalty Mechanism for Inaccurate Participation
V. Data Privacy and Security Measures

Candidate Verification and Consent

Upon receiving a notification, the candidate reviews the details to determine if the background check request pertains to them. They verify the employer's identity and legitimacy to ensure they are responding to a valid request. If the candidate recognizes the request as intended for them, they decide to proceed; if not, they can choose to ignore it without any penalty.

Granting Temporary Access

To proceed, the candidate confirms their identity, typically by signing the response with their private key or using multi-factor authentication methods, and provides explicit consent for the background check to continue. They generate a temporary access key or token that allows the employer to access their encrypted background information for a limited time. This access key is securely transmitted to the employer, often encrypted with the employer's public key to ensure that only they can use it. The candidate can specify the scope of information the employer can access,

such as specific records or time periods. Access is granted for a predefined duration, after which the employer can no longer access the data without further consent.

Reward Mechanism for Accurate Participation

Candidates receive rewards in the form of tokens or credits for accurately confirming their identity and participating in the background check process. These rewards are provided promptly after the candidate completes the necessary steps, encouraging timely responses. Rewards are contingent upon the accuracy of the candidate's background information, and prompt responses within the 24-hour notice period may result in higher rewards. Successful verification of the candidate's background information can enhance the reward amount.

Penalty Mechanism for Inaccurate Participation

To discourage fraudulent behavior, candidates who provide false information or inaccurately confirm an identity that is not theirs are subject to penalties. Penalties may include token deductions, temporary suspension from the network, or reductions in reputation score. The employer, upon accessing the candidate's information, can report discrepancies or inaccuracies. A dispute resolution process is in place to handle such issues, allowing candidates to contest penalties if they believe they are unjustified. Penalties are enforced transparently, with records maintained on the blockchain to ensure fairness.

Data Privacy and Security Measures

The candidate's background information remains encrypted and secure, accessible only with the temporary access key. Personal data is not exposed on the blockchain; only necessary information is shared with authorized parties. Communication between the candidate and employer is secured using cryptographic protocols, and temporary access keys are transmitted securely to prevent interception or unauthorized use. The system complies with relevant data protection and privacy regulations, such as GDPR or CCPA, ensuring that candidates have control over their data and can revoke consent as necessary.

Step 4: No Response Protocol

These steps outline the procedures that occur when a candidate does not respond to a background check request within the designated 24-hour period. A designated researcher node steps in to ensure the background check process continues smoothly, maintaining the system's efficiency and reliability.

Key Components:

I. Detection of Non-Response
II. Authorization of Researcher Node
III. Access Permissions for Researcher
IV. Privacy and Security Considerations

Detection of Non-Response

The system tracks the time elapsed since the background check request was submitted, initiating a 24-hour countdown when the request is added to the blockchain. If no candidate matching the hashed information responds within this 24-hour window, the system recognizes a non-response event.

Authorization of Researcher Node

In cases of non-response, researcher nodes—pre-approved entities within the network authorized to conduct background checks when candidates do not respond—are activated. These researchers are trusted parties, certified by the network's governing body. Upon detecting a non-response, the system automatically assigns the request to an available researcher node, and an assignment transaction is recorded on the blockchain to indicate the researcher's authorization to proceed.

Access Permissions for Researcher

The researcher node is granted permissions to access the necessary data to compile the background check, with data access strictly controlled and limited to what is necessary. The system may generate a temporary access key for the

researcher, similar to the key a candidate would have provided, allowing the researcher to decrypt or retrieve the required information securely. Researchers are bound by legal agreements and network policies to handle data responsibly, and any access to data is logged and monitored to ensure compliance.

Privacy and Security Considerations

To protect privacy, researchers access only the minimum amount of data necessary to perform the background check. Personal identifiers are handled with care to prevent unnecessary exposure, and all data transmission between the network and researcher nodes is encrypted. The system maintains detailed logs of data access by researcher nodes for accountability.

Advantages of the No Response Protocol

This protocol ensures continuity by allowing employers to receive background check results even if the candidate does not respond. It minimizes delays in the hiring process, enhancing timeliness, and maintains system integrity by demonstrating the system's ability to handle exceptions effectively.

Step 5: Researcher Compiles and Delivers Results

Enable the researcher to compile the background check report using authorized access and deliver the results to both the employer and the candidate, with mechanisms in place for contestation if necessary.

Key Components:

I. Data Collection and Compilation
II. Report Generation
III. Delivery of Results
IV. Contestation Mechanism
V. Privacy and Security Considerations

Data Collection and Compilation

The researcher uses the temporary access permissions to retrieve relevant background information about the candidate. Data sources include public records, previous employment verifications, education credentials, and any other pertinent information. Throughout this process, the researcher ensures that all data collected complies with legal standards and regulations.

Report Generation

After collecting the necessary data, the researcher reviews and analyzes the information to create an accurate background check report. The report typically includes identification verification, employment history, education verification, criminal records check (if applicable), and other relevant findings. Before delivery, the report is checked for accuracy and completeness to ensure quality.

Delivery of Results

The background check report is securely transmitted to both the employer and the candidate using encryption methods to protect the data during transmission. Both parties receive notifications that the report is available. The report can be accessed through secure portals requiring authentication, ensuring that only authorized individuals can view the information.

Contestation Mechanism

Upon receiving the report, the candidate has the opportunity to review it and identify any inaccuracies, while the employer reviews the report to make informed decisions. If discrepancies are found, either the candidate or the employer can submit a formal dispute. A predefined dispute resolution process is in place, which may involve verification of disputed information, correction of errors in the report, or re-evaluation by a different researcher or an independent arbitrator. Specific timeframes are established for submitting disputes and resolving them to ensure the process remains efficient.

Privacy and Security Considerations

Personal data within the report is protected according to data protection laws and regulations. All parties involved are subject to confidentiality obligations to prevent unauthorized disclosure. The entire process is subject to audits to ensure compliance with policies and regulations, maintaining the integrity and security of the information.

Advantages of the Researcher Compilation and Delivery Process

This process ensures employers receive the necessary background information, facilitating the hiring process. It keeps candidates informed and involved, even if they did not initially respond. The contestation mechanism allows for corrections, ensuring fairness and transparency throughout the process.

Potential Challenges and Mitigations:

I. **Data Accuracy Concerns**

Challenge: There is potential for errors in the report due to outdated or incorrect data sources.

Mitigation: Researchers use reputable and up-to-date sources. The contestation mechanism allows for the correction of any inaccuracies identified by the employer or candidate.

II. **Privacy Breaches**

Challenge: There is a risk of sensitive information being exposed during the process.

Mitigation: Strict access controls and encryption are implemented. Regular security audits and adherence to best practices help protect sensitive data.

III. **Dispute Resolution Delays**

Challenge: Prolonged disputes may delay hiring decisions.

Mitigation: Clear timelines and efficient processes for dispute resolution are established. Technology is used to streamline verification and correction steps to expedite the process.

Role of Researchers

Researchers are trusted entities with expertise in conducting background checks. They operate under strict guidelines to ensure legal and ethical compliance and are accountable for the accuracy and integrity of the reports they produce. Their expertise and trustworthiness are crucial for maintaining the system's reliability.

Ethical and Legal Compliance

Even if the candidate did not respond initially, they are notified of the background check results and have the opportunity to contest any inaccuracies. The process complies with laws such as GDPR, ensuring that data is handled lawfully and ethically. The background check process is designed to prevent discriminatory practices, promoting fairness and equality for all candidates.

Step 6: Contestation Mechanism

Allows both employers and candidates to dispute the contents of the background check report if inaccuracies or discrepancies are found. This mechanism is crucial for maintaining fairness, accuracy, and trust within the system. It provides a structured process for resolving disputes, ensuring that all parties have the opportunity to correct errors and that the integrity of the background check is upheld.

Key Components:

I. Initiation of a Dispute
II. Submission of Dispute to the Network
III. Dispute Resolution Mechanism
IV. Roles and Responsibilities
V. Timeframes and Deadlines
VI. Outcome Implementation

Initiation of a Dispute

Upon receiving the background check report, both the employer and the candidate independently review its contents to check for any inaccuracies, discrepancies, or information that may be outdated or incorrect. Grounds for contestation may include inaccurate personal information, incorrect employment history, erroneous criminal records, or any data that the party believes is incorrect or misrepresented. The party assesses whether these inaccuracies significantly impact the report's conclusions or decisions before deciding to initiate a dispute.

Submission of Dispute to the Network

To formally contest the report, the disputing party initiates the contestation process by submitting a formal dispute to the network. This submission includes their identification (employer or candidate), specific references to the sections of the report being contested, supporting documentation or evidence that substantiates the claim of inaccuracy, and a clear and concise explanation of the issue. The dispute is submitted through a secure channel to protect sensitive information. Upon receipt, the network acknowledges the dispute and provides a reference number for tracking.

Dispute Resolution Mechanism

Once the dispute is submitted, the network verifies that the submission is complete and valid and notifies the other party of the dispute, providing them with the details. An impartial arbitrator or review panel is appointed to review the dispute, selected based on expertise, neutrality, and absence of conflict of interest. The arbitrator collects all relevant information from both parties and may request additional data from the researcher or external sources as needed. They examine the evidence provided, ensuring that the resolution complies with legal standards and network policies. Based on the evidence, the arbitrator reaches a decision, which may result in correction of the report, dismissal of the dispute if unfounded, or additional actions such as penalties if misconduct is found. Both parties are informed of the decision and any actions to be taken, and if corrections are made, an updated report is issued to both parties.

Roles and Responsibilities

The disputing party must supply accurate and relevant information to support the dispute and respond promptly to requests for additional information. The other party may provide counter-evidence or statements and assist in the resolution process as required. The arbitrator or review panel must remain impartial throughout the process, conduct a thorough investigation, consider all evidence, and aim to resolve the dispute within the established timeframes. The network administration ensures that the contestation mechanism functions smoothly and maintains records of disputes and outcomes for accountability.

Timeframes and Deadlines

Parties have a specified period, such as seven days from receipt of the report, to submit a dispute. The arbitrator aims to resolve the dispute within a set timeframe, for example, 14 days. Extensions may be granted in complex cases, with notifications provided to both parties.

Outcome Implementation

If corrections are necessary, the report is amended to reflect accurate information, and an updated report is sent to both parties. The outcome is recorded on the blockchain, ensuring transparency and immutability while protecting sensitive details by recording only necessary information publicly. If deliberate misinformation is identified, penalties may be applied to the responsible party, and adjustments to reputation scores may impact their standing in the network.

Security and Privacy Considerations

All communications during the dispute process are encrypted to ensure confidentiality, and personal and sensitive information is handled in compliance with data protection regulations. The blockchain ensures that records of the dispute and its resolution are immutable, and digital signatures and authentication verify that submissions are genuine. To ensure fairness, arbitrators are selected to be neutral and unbiased, and the process is transparent with clear procedures and criteria.

Incentive and Penalty Mechanisms

Incentive Mechanism Details

We propose the exponential decay formula for the rewards will be as follows:

$$T(t) = 100 \times e^{-\lambda t}$$

where:

- ➔ 100 is the initial token reward count,
- ➔ λ is the decay constant,
- ➔ t is time elapsed in hours.

Purpose: Encourage candidates to participate honestly and promptly.

Token Utility: Tokens can be used within the network for services, transferred to others, or possibly converted to other currencies.

Penalty Mechanism Details

We propose for the token penalty to always be the equivalent of max value of the rewards.

Purpose: Deter fraudulent behavior and maintain system integrity.

Penalty Triggers: Providing false information, misrepresenting identity, or other dishonest actions.

Penalty Severity: Proportional to the severity of the infraction; repeat offenses may incur harsher penalties.

Appeals Process: Candidates can appeal penalties through a formal dispute resolution mechanism.

Data Onboarding

Data onboarding is a crucial step in integrating users and their information into the blockchain-based background check system. It involves the systematic addition of both historical and new data to create comprehensive and up-to-date profiles for users. This process ensures that background checks are accurate, reliable, and reflective of the most current information available.

Previous History Onboarding

Existing records from trusted institutions can be onboarded onto the blockchain to provide a solid foundation for accurate background checks. This historical data includes past employment records, educational qualifications, certifications, licenses, and any other pertinent information that reflects a user's professional and personal history. By integrating these existing records, the system leverages verified information from reputable sources, enhancing the credibility and depth of the background checks. The onboarding of previous history not only streamlines the verification process for employers but also empowers users by showcasing their established credentials and experiences.

New History Onboarding

As users progress in their careers, gain new skills, or acquire additional qualifications, they can continuously add this information to the blockchain. Each new entry undergoes a verification process by the relevant authorities or institutions to ensure its authenticity. Once verified, the information is timestamped and securely added to the user's blockchain profile. This ongoing updating mechanism maintains an accurate and current profile for each user, reflecting their latest achievements and experiences. It allows for dynamic background checks that can adapt to the user's growth over time, providing employers with the most recent information and enabling users to keep their professional profiles up-to-date.

New User Onboarding

When new users join the system, they begin with the identity verification process to establish their unique blockchain identity. They provide essential details such as their full legal name, birthdate, and place of residence. This personal information is securely hashed to protect their privacy and linked to their blockchain identity, ensuring that their sensitive data remains confidential.

The system then assesses the status of their records:

I. **Existing Records**: If the new user has existing records from previous employment, educational institutions, or certifications, these records are linked to their profile after thorough verification. This linkage helps in creating a comprehensive background profile, allowing the user to benefit from their past experiences and qualifications immediately.

II. **No Records**: For users without prior records, perhaps recent graduates or individuals entering the workforce for the first time, the system establishes a new blockchain identity. These users start with a clean slate and can begin building their background profile as they acquire employment, education, or other credentials. The system provides a secure platform for them to accumulate verified records over time.

III. **Records to be Added**: Users may have new or additional records that are not yet part of the blockchain. They can submit these records, such as recent certifications, new degrees, or updated contact information, which are then subjected to a verification process. Once authenticated, these records are added to the blockchain, enhancing the user's profile with the latest information.

By facilitating both the onboarding of previous history and the continuous addition of new data, the system ensures that all user profiles are accurate, verified, and current. This comprehensive approach to data onboarding strengthens the overall effectiveness of the background check system, benefiting both employers seeking reliable information and users aiming to present their qualifications authentically.

Node Types

In the blockchain-based background check system, nodes are central to maintaining network functionality, security, and efficiency. Each node type—Requester Nodes, Candidate Nodes, and Researcher Nodes—has specific responsibilities, operating under protocols that ensure seamless interaction among participants. This architecture facilitates a secure, decentralized, and transparent system for background checks.

Node Types Overview

Requester Nodes are operated by employers or entities initiating background checks. Candidate Nodes are managed by individuals subject to the checks, allowing them to monitor requests and control their data. Researcher Nodes are run by authorized researchers who compile reports when candidates fail to respond within a specified timeframe.

I. Requester Nodes

These nodes enable employers to initiate background checks by hashing candidates' personal information and submitting it to the blockchain. Requester Nodes manage transaction creation, including data hashing and submission, while monitoring candidate responses. In cases of non-response, these nodes activate the No Response Protocol, engaging Researcher Nodes for report compilation. Employers receive results securely through encryption and access keys, ensuring compliance with data protection laws.

II. Candidate Nodes

Candidates use these nodes to monitor requests, respond, and manage personal data. The node continuously scans for matching transactions, notifying the candidate of requests. Candidates verify the legitimacy of requests, grant consent, and provide temporary access keys to employers. They can also update profiles, control data privacy, and receive rewards for timely participation. Candidate Nodes emphasize secure key management, data encryption, and compliance with privacy laws.

III. Researcher Nodes

When candidates do not respond, Researcher Nodes compile reports to ensure employers receive necessary information. These nodes access authorized data, analyze it for accuracy, and securely deliver reports to both employers and candidates. Researcher Nodes follow strict encryption protocols, maintain access logs, and adhere to ethical standards. They also assist in resolving disputes and ensuring compliance with regulatory requirements.

Node Communication and Protocols

All nodes interact through blockchain transactions to ensure transparency and security. Key transactions include background check requests, candidate responses, researcher assignments, and dispute submissions. Security is maintained through encryption standards, public-private key cryptography, and strict access controls. Compliance with data protection laws and a governance framework ensures accountability and transparency.

Benefits and Challenges

The decentralized architecture distributes responsibilities, enhancing scalability, security, and transparency. Automated protocols streamline the process, while blockchain technology secures data and fosters trust. Challenges such as synchronization issues, data privacy concerns, and node reliability are mitigated through consensus mechanisms, advanced encryption, and redundancy strategies.

Broadcasting Intent Status

In the blockchain-based background check system, effective communication of a candidate's availability and expectations is essential for streamlining the verification process. Broadcasting Intent Status allows candidates to indicate their current status regarding background checks, which aids researchers and employers in efficiently identifying and processing the correct candidates. This chapter explores the concept of Broadcasting Intent Status, defines specific statuses, and explains how this mechanism enhances the overall efficiency and accuracy of the background check system.

Overview of Broadcasting Intent Status

Broadcasting Intent Status is a feature that enables candidates to publicly share their current stance or expectations concerning background checks within the blockchain network. By broadcasting this information, candidates help researchers and employers understand whether they should anticipate a background check request or if there are any specific considerations to be aware of. This proactive communication reduces unnecessary inquiries and expedites the verification process.

Purpose and Benefits

The Intent Status mechanism is a pivotal feature within the blockchain-based background check system, designed to enhance efficiency, accuracy, transparency, and resource optimization. By allowing candidates to communicate their current availability and expectations regarding background checks, the system helps researchers and employers quickly identify candidates who are ready and expecting a background check, thereby reducing processing time. This proactive communication minimizes the chances of incorrect candidate identification by providing additional context, ensuring that the right individuals are engaged promptly.

Transparency is significantly enhanced as candidates openly communicate their intentions, fostering trust within the system. This openness allows the network to allocate resources effectively, focusing on candidates prepared for the background check process. By streamlining interactions, the system not only improves efficiency but also empowers candidates to have control over their engagement, contributing to a more effective and user-centric background check process.

Defined Intent Status Categories

Candidates can select from predefined statuses that best represent their current situation, each with specific meanings and implications for the background check process:

1. **Available for Background Check**: This status indicates that the candidate is actively seeking employment or opportunities and expects background check requests. The implications are significant for priority processing, as researchers and employers know the candidate is ready, allowing for expedited handling. Open communication is facilitated, with the candidate likely to respond promptly to notifications, streamlining the hiring process.
2. **Not Expecting Background Check**: When a candidate is not currently seeking new opportunities and does not anticipate any background check requests, this status helps the system reduce unnecessary notifications to the candidate. Researchers understand that the candidate may not respond promptly, and alternative protocols may be necessary, respecting the candidate's current professional stance.
3. **Pending Background Check**: This status signifies that the candidate is aware of an upcoming background check request and is prepared to respond. The implications include immediate attention from researchers and employers, signaling readiness for immediate processing. It also reinforces that any received requests are expected and legitimate, smoothing communication channels.
4. **Do Not Disturb**: When a candidate is temporarily unavailable and prefers not to receive background check requests during a specified period, this status ensures that the system temporarily suspends notifications to the candidate. Researchers may note this status and schedule follow-ups accordingly, respecting the candidate's need for temporary unavailability and fostering goodwill.

5. **Verification in Progress**: Indicating that the candidate is currently undergoing a background check process, this status helps prevent duplication by alerting employers and researchers. They can track the progress and anticipate completion, avoiding unnecessary parallel processes and respecting the candidate's ongoing engagements.
6. **Request Additional Information**: This status is used when the candidate requires more information before consenting to a background check. It signals to employers that clarification is needed, promoting enhanced communication and direct engagement to address any concerns or questions the candidate may have.

Implementation of Intent Status

Candidates can set their Intent Status through their Candidate Node interface or user dashboard, providing a user-friendly way to update their status at any time. They may set durations for certain statuses, such as "Do Not Disturb" for one week, offering flexibility and control over their availability. Changes in status can trigger notifications to relevant parties, such as previous employers or potential recruiters, ensuring that all stakeholders are informed of the candidate's current intentions.

The visibility of the Intent Status is managed through access control, making it visible only to authorized researchers and employers within the network. Privacy considerations are integral; only the status is shared without disclosing personal details, and candidates have full control over their status visibility, with the option to opt out if desired.

Impact on Researchers and Employers

The Intent Status mechanism streamlines candidate identification by allowing researchers to filter candidates based on their status, focusing on those who are available or pending. This reduces false positives and the likelihood of contacting the wrong candidate. Processing protocols can be adjusted accordingly; for example, if a candidate's status is "Not Expecting Background Check" or "Do Not Disturb," researchers can modify their approach, perhaps delaying outreach or preparing alternative strategies.

Enhanced communication is facilitated as employers can tailor their interactions based on the candidate's Intent Status. Acknowledging statuses like "Do Not Disturb" fosters goodwill and professionalism, respecting candidate preferences and contributing to a positive relationship between all parties involved.

Use Cases and Scenarios

- **Scenario 1: Active Job Seeker**

  A candidate sets their status to "Available for Background Check." The outcome is that the candidate receives background check requests promptly and responds quickly, facilitating a smooth hiring process.
- **Scenario 2: Passive Candidate**

  With a status of "Not Expecting Background Check," employers recognize that the candidate may require additional outreach or incentives to engage, adjusting their strategies accordingly.
- **Scenario 3: Temporary Unavailability**

  When a candidate selects "Do Not Disturb," researchers postpone background check activities, respecting the candidate's unavailability and scheduling follow-ups as appropriate.
- **Scenario 4: Multiple Offers**

  A candidate indicates "Verification in Progress," signaling to employers that they are already undergoing a background check elsewhere. Employers can decide to wait or proceed accordingly, avoiding duplication and respecting the candidate's ongoing processes.

Technical Considerations

Integration with Candidate Nodes is essential for implementing the Intent Status mechanism effectively. A status management interface provides a user-friendly way for candidates to update their status, and automatic status updates can be configured based on specific triggers, such as accepting a job offer.

Data storage and privacy are carefully managed. Intent Status changes are recorded on the blockchain to ensure transparency and immutability, while encryption protects status information from unauthorized access. Compliance with regulations like GDPR is maintained, ensuring that updating Intent Status does not override the need for explicit consent for background checks and that broadcasting status does not infringe on privacy rights.

Best Practices for Candidates

Candidates are encouraged to keep their Intent Status current to reflect their true availability and expectations. Clear communication through accurate status descriptions helps prevent misunderstandings, and candidates should be aware of how their status information is used and who can access it, maintaining control over their privacy.

Benefits to the Background Check System

The Intent Status mechanism enhances accuracy by helping match background check requests with the correct candidates. It improves efficiency by reducing unnecessary processing and follow-ups, allowing the network to allocate efforts where they are most needed. Candidate empowerment is promoted by giving individuals control over their engagement with the system, contributing to a more user-centric and effective background check process. Overall, resource optimization is achieved, improving the system's performance and reliability.

ERC-20 Token

The **Foreground Network (FGN)** token serves as a precursor to the mainnet fungible utility token that the network will employ once it becomes fully operational. Currently deployed as an ERC-20 token, FGN will be exchangeable on a one-to-one basis with the forthcoming mainnet token, allowing holders to seamlessly transition once the network launches. These tokens can be redeemed or exchanged at any time, ensuring flexibility and ease of involvement for early participants.

To differentiate this ERC-20 implementation from the many generic tokens that have eroded trust in the past, the contract integrates a variety of read-only functions and placeholders. These features offer stakeholders a transparent preview of the network's intended functionality, while also discouraging the deceptive practices seen in basic, unremarkable ERC-20 contracts. By providing this initial, carefully structured token with a total supply of 100 million units, the **Foreground Network (FGN)** aims to foster a community of informed, confident participants who can engage with its evolving ecosystem securely and with clear expectations.