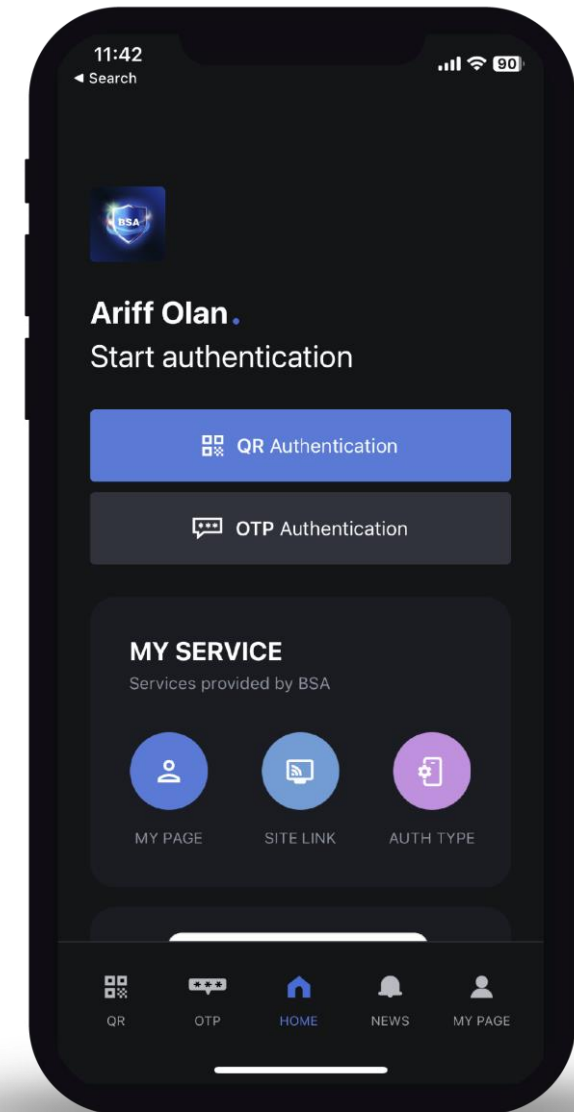




Passwordless Blockchain Secure Authentication

Technology Overview



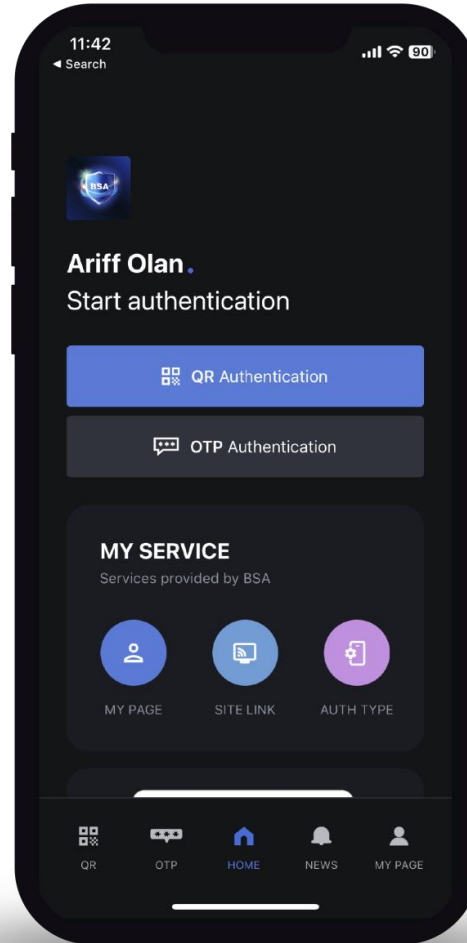
Introduction







What is Passwordless BSA?

A **True-Passwordless Multifactor Authentication (MFA)** Solution

Utilizes **Blockchain Technology** for verification & authentication.



Unique Technologies

-  Multiple Identifier Random Combination (MIRC)
-  One-Time Security Key (OTSK)
-  Multilateral Distributed Verification (MDV)
-  Kernel Chain Core (KNChain) Hybrid Blockchain

How Passwordless BSA works?

Passwordless BSA works on 3 levels:



If any of the steps fail, the user will be unable to advance to the next level.

Onboarding Process

Upon onboarding, users will:

1. Provide only 4 unique information:
 - i. Full Name
 - ii. Username
 - iii. Email address
 - iv. Mobile number
2. Register one mobile device to act as authenticator
3. Registered users will become a blockchain node which will be used for blockchain authentication

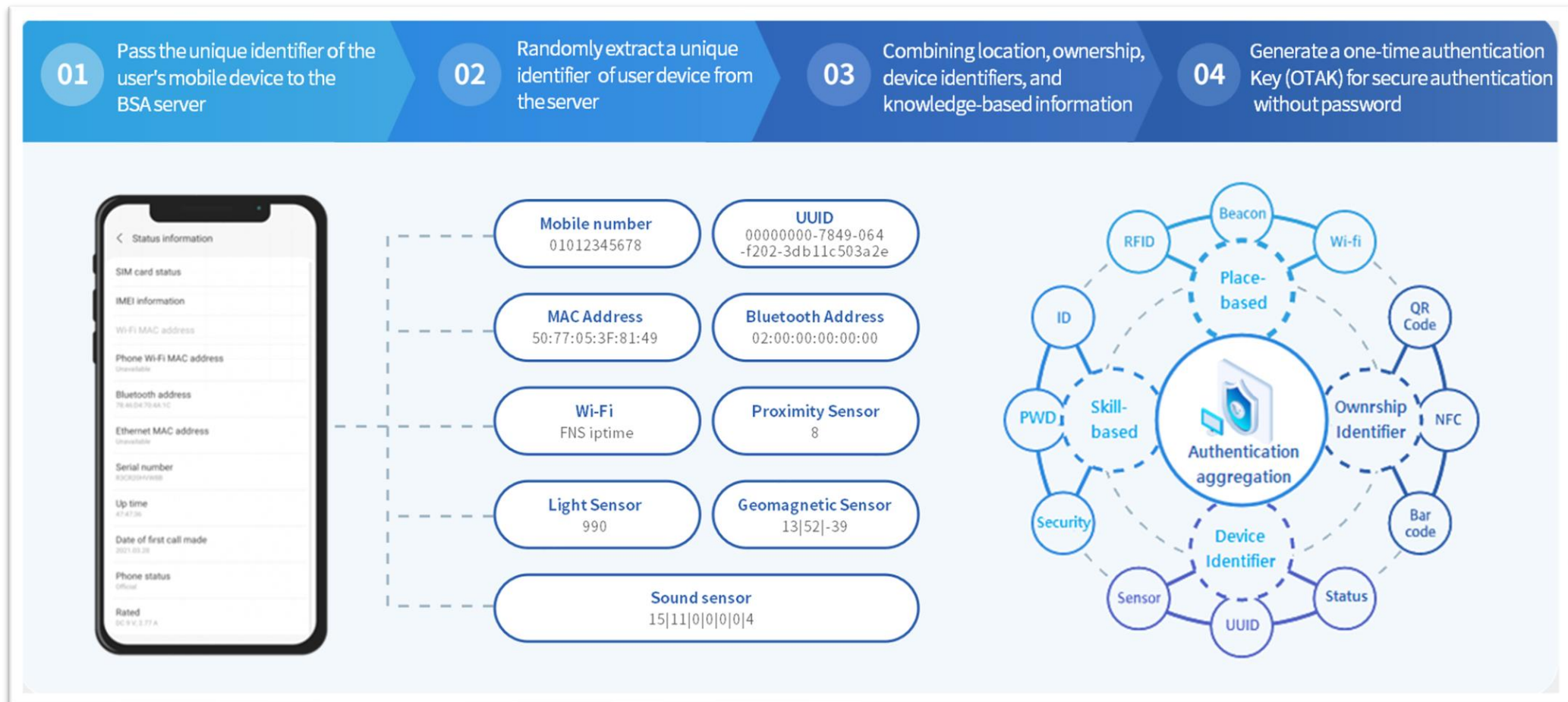


Level 1: Device



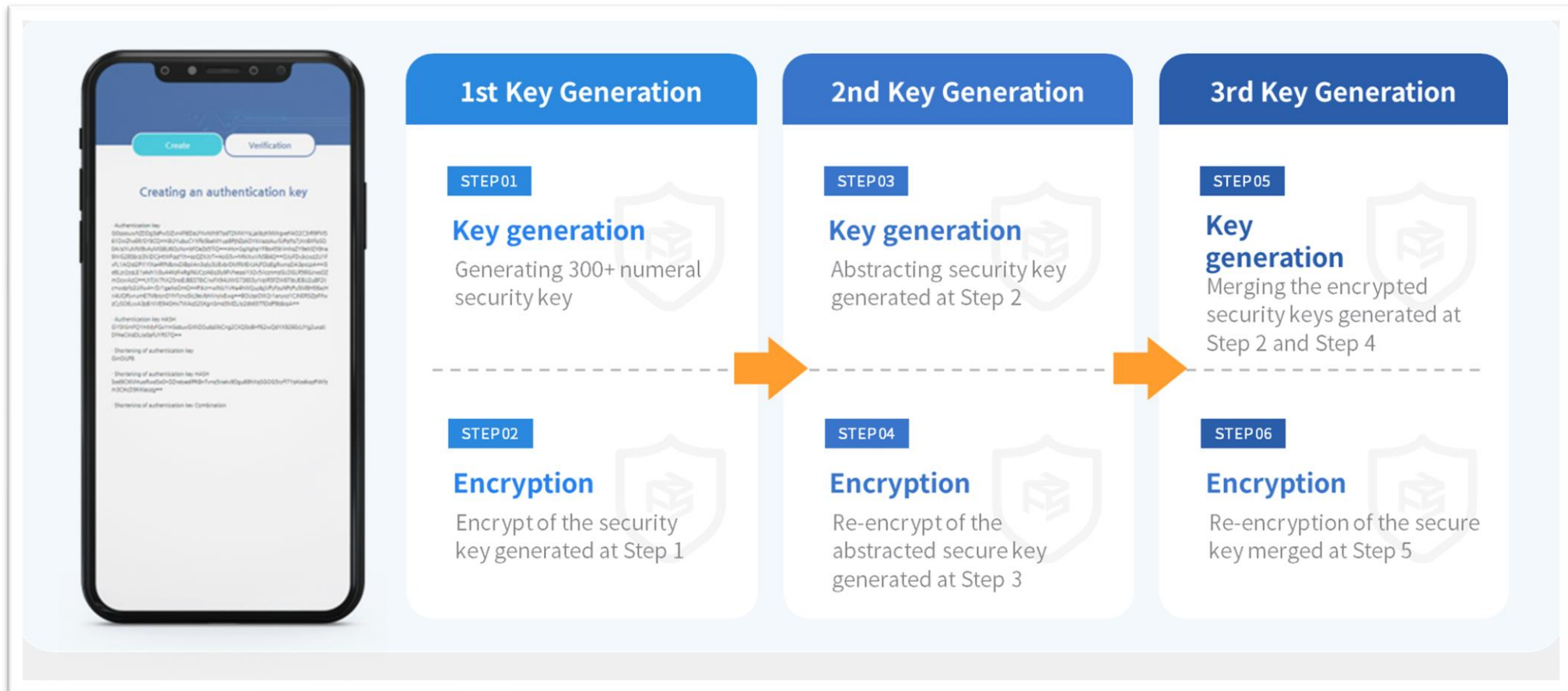
Level 1: Device Multi Identifier Random Combination (MIRC)

Extract multiple unique identifiers from users' mobile devices to create unhackable unique key.

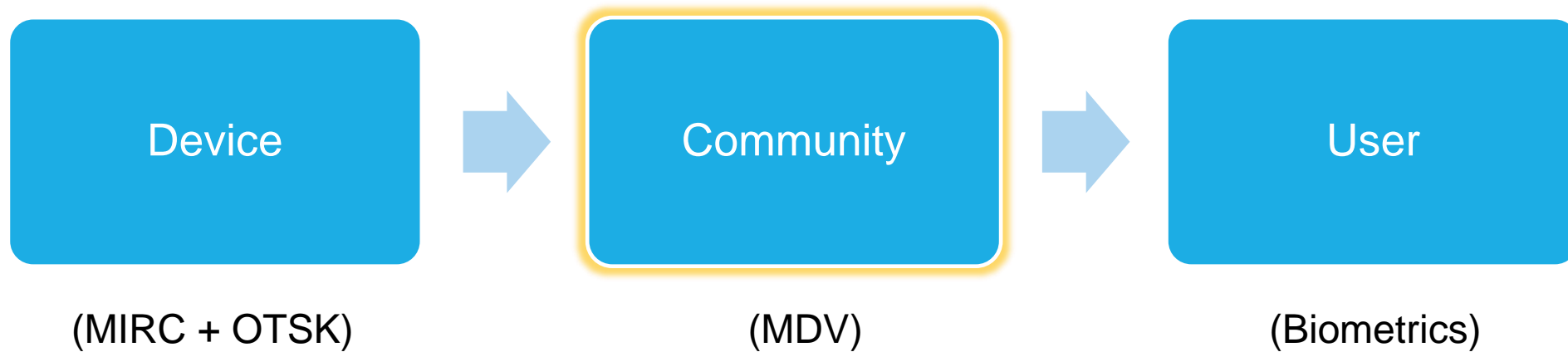


Level 1: Device One-Time Authentication Key

BSA used one time authentication key for blockchain for blockchain channel, block and instances to eliminate a single point of forgery during authentication process. OTAK is 100% volatile and unhackable.

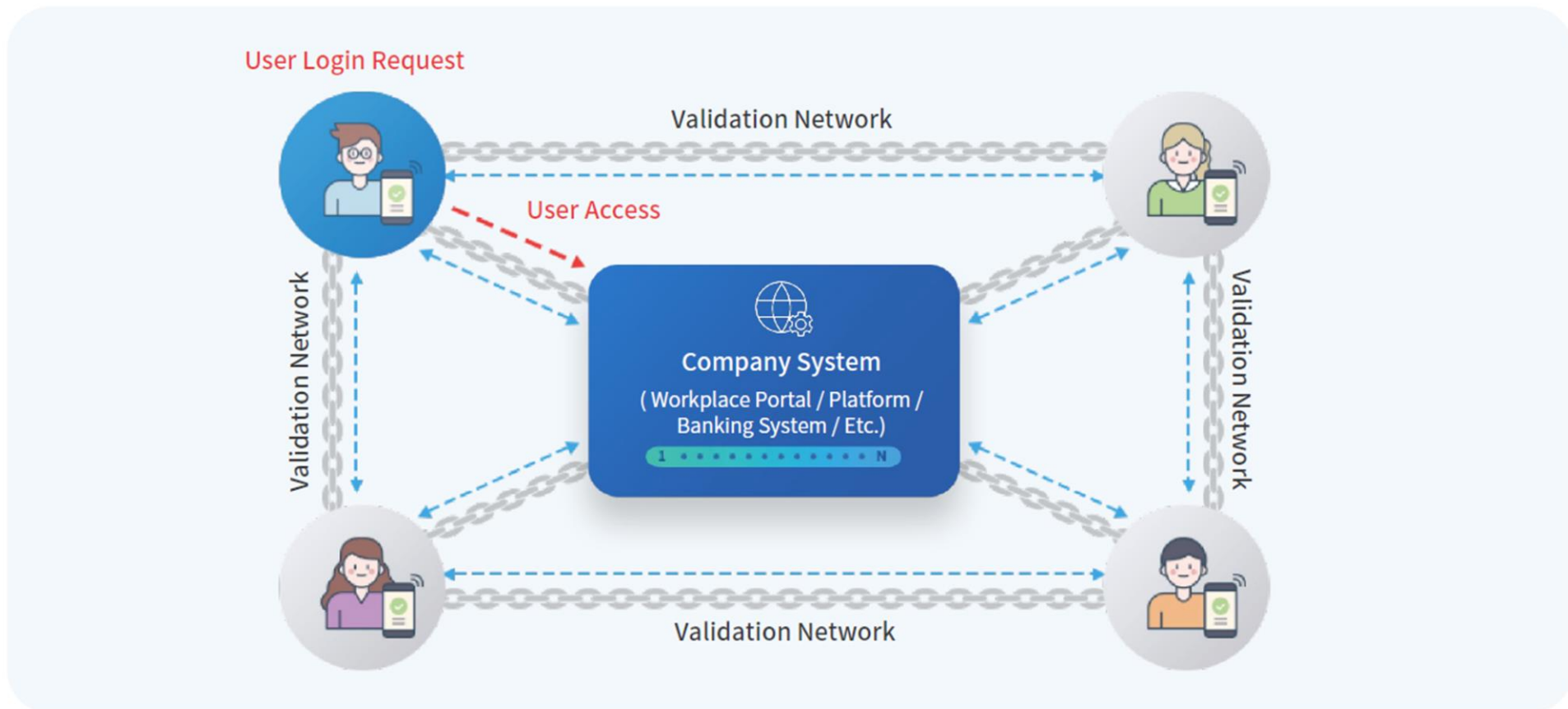


Level 2: Community



Level 2: Community Multilateral Distributed Verification (MDV)

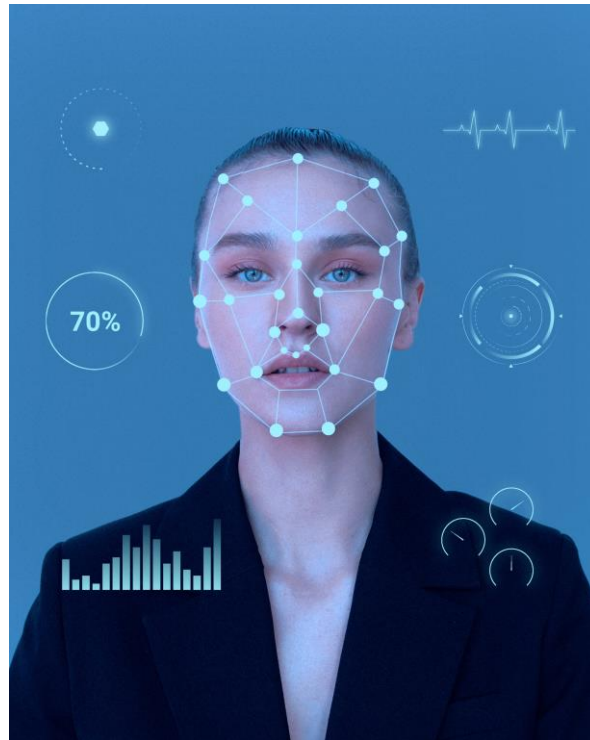
BSA applies multiple distributed verification technologies to its own KNChain to maximize security levels



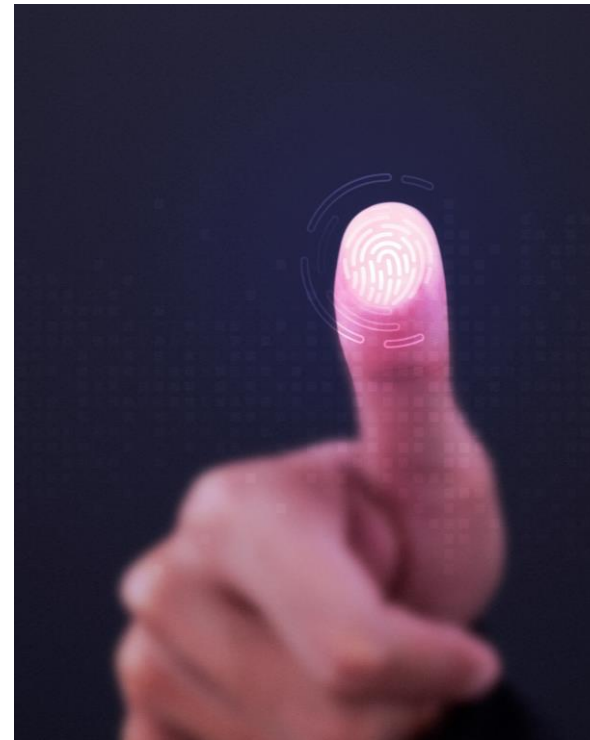
Level 3: User



Level 3: User Biometrics



Face ID



Fingerprint

Note: Type of biometrics is dependent on the user's mobile phone capabilities.

Kernel Chain Network (KNCHAIN) Hybrid Blockchain Network

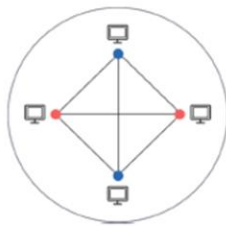
New global authentication ecosystem for individuals and corporation. Fast, easy, and strong secure authentication service.
Hybrid blockchain service independent technology

Public Blockchain



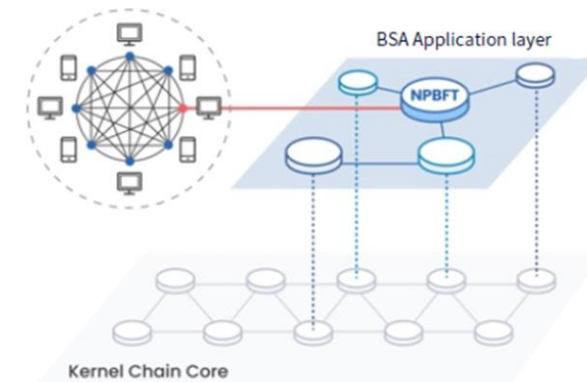
- Network configuration in the form of voluntary and unrestricted participation.
- Open blockchain (public blockchain).
- Individual devices such as computers and mobile phones that participate in the network are called nodes.
- Free participation and open technology to all user.

Private Blockchain



- Network configuration with restricted access limited which allowed only designated user to participate
- Mainly used by banks and public institutions
- It operates with a limited number of nodes, allowing only authorized users to participate as nodes, unlike public blockchains.
- A Private Blockchain is integrated into the core authentication processing area of a Public Blockchain to enhance security in the authentication processing domain.

Hybrid Blockchain



- ✓ Network configured to maximize advantages of public and private blockchain
- ✓ Provides key features such as security, immutability, transparency, and decentralization
- ✓ User anonymity is limited, but public anonymity is maintained, so no one outside the network knows the blockchain user



Solution Demonstration





BSA

PASSWORDLESS

Use Cases

Passwordless BSA is applicable for the following use cases:

1. Managing Policies
2. Secured Application Login
3. Secured Payment Approval
4. Secured Virtual Private Network (VPN)
5. Secured Document Retrieval
6. Secured Digital Signing



Passwordless BSA Setup

Passwordless BSA can be set up in two ways:



Passwordless BSA On-Cloud

- On-Cloud Security as a Service (SaaS) for both public and private customers.



Passwordless BSA On-Premise

- Provide On-Premise Security as a Service (SaaS) for customer web and mobile applications.
- One-off BSA per site license with unlimited applications.

Note: All Services are on a yearly subscription basis based on per user license.



Other Services

Here are other services that the technology principal has to offer:



Consulting

- Project Management Services
- Systems Integration Services
- Deployment & Services Delivery
- API Development & Customisation
- SDK & Plugins Development & Customisation



Value Added Services

- eKYC
- Digital Certificate
- Digital Signature



Targeted Industries

Here are examples of our targeted industries:

Financial Institutions

- Protect from unauthorized access or tampering – Bank Negara revised RMIT, regulated to comply with highest level of authentication possible



Government

- Protect government data from unauthorized access and tampering – many government assets and data is sold to dark web due to weak authentication



Information & Communications

- Protect privacy of data through decentralization to secure from unauthorized access – comply to PDPA



Healthcare

- Protect access to critical data – cannot be protected with current centralized way of authentication





Q&A



**Passwords are a thing of the past, the
future is passwordless.**



Thank you.