Efficient Key Management Scheme for Health Blockchain

Paper review

https://youtu.be/NXwijDHKAYU

H. Zhao, P. Bai, Y. Peng and R. Xu, "Efficient key management scheme for health blockchain," in *CAAI Transactions on Intelligence Technology*, vol. 3, no. 2, pp. 114-118, 6 2018.

Blockchain

- Is consists of
  - Consensus Mechanism
  - Digital Signature
  - Hash Chains
  - Shared Database

Blockchain

- Provides
  - Non-Repudiation
  - Integrity
  - Distributed Storage
  - Time-based Traceability

Blockchain

- Can be used in
  - Healthcare
  - Fintech
  - Computational Law
  - Audit
  - Notarization

Blockchain

- Has
  - Speed of recording Issue
  - Efficiency of consensus Issue
  - Privacy of data Issue

Privacy of Data

- ~~Zero-Knowledge Proof~~

- Encrypt and Store
  - Key Management Issue

Key Management Issue

- One key for all blocks

- One key for a block

+
Considering application scenario

Health Blockchain

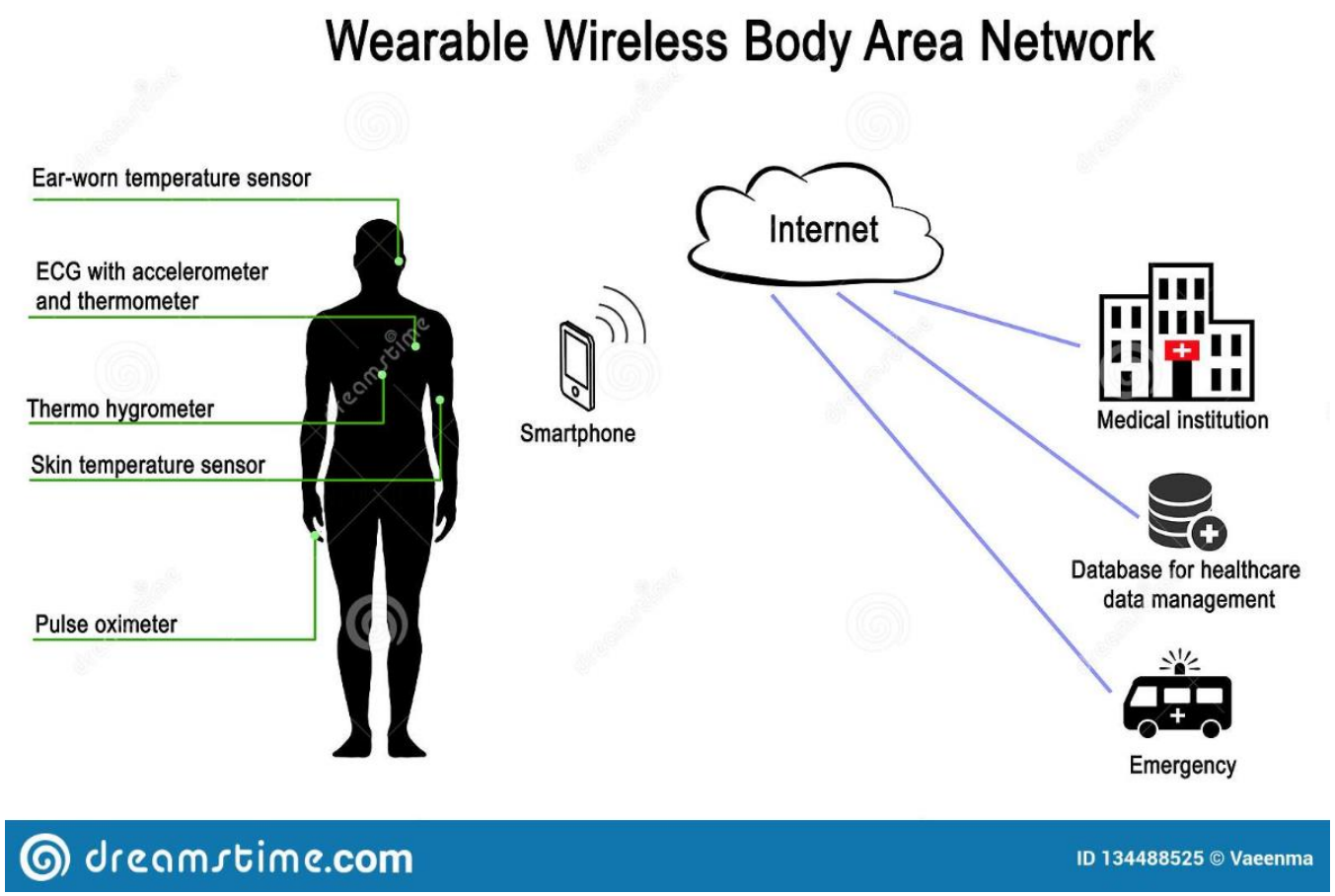
- Blockchain handling health data

- Has a number of private data

→ Must solve privacy issue

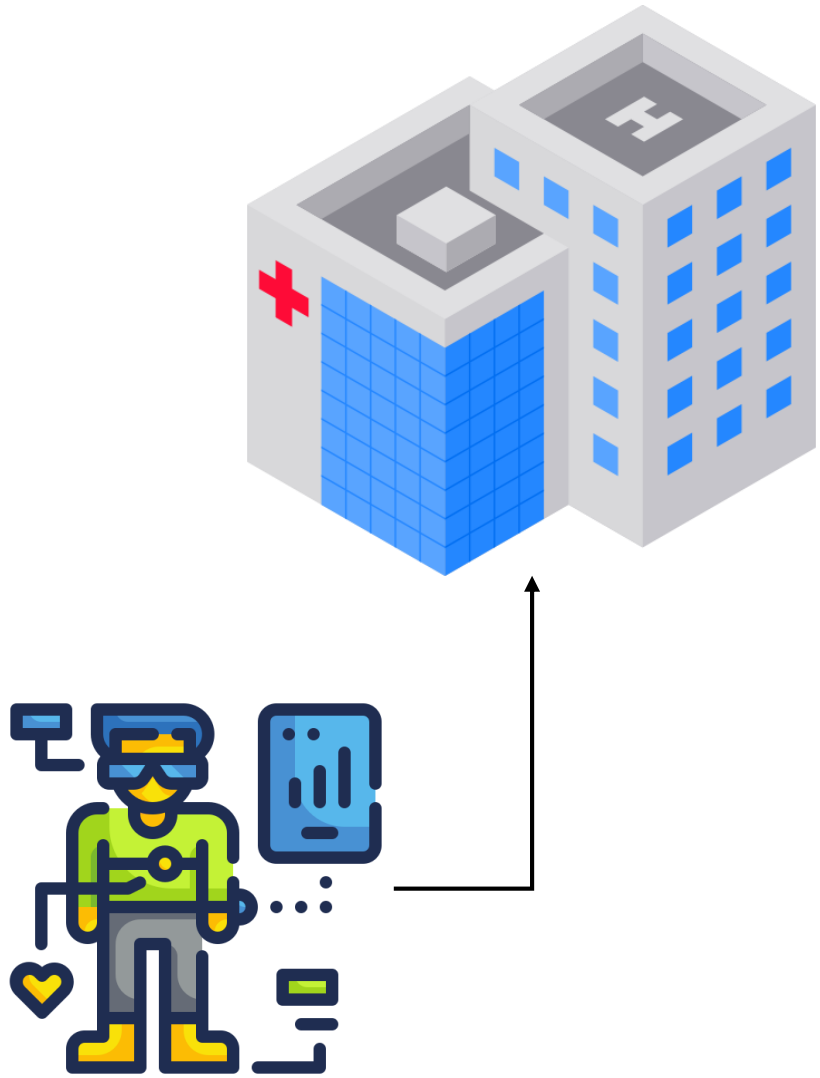
Body Sensor Networks (BSNs)

- BAN, WBAN, MBAN



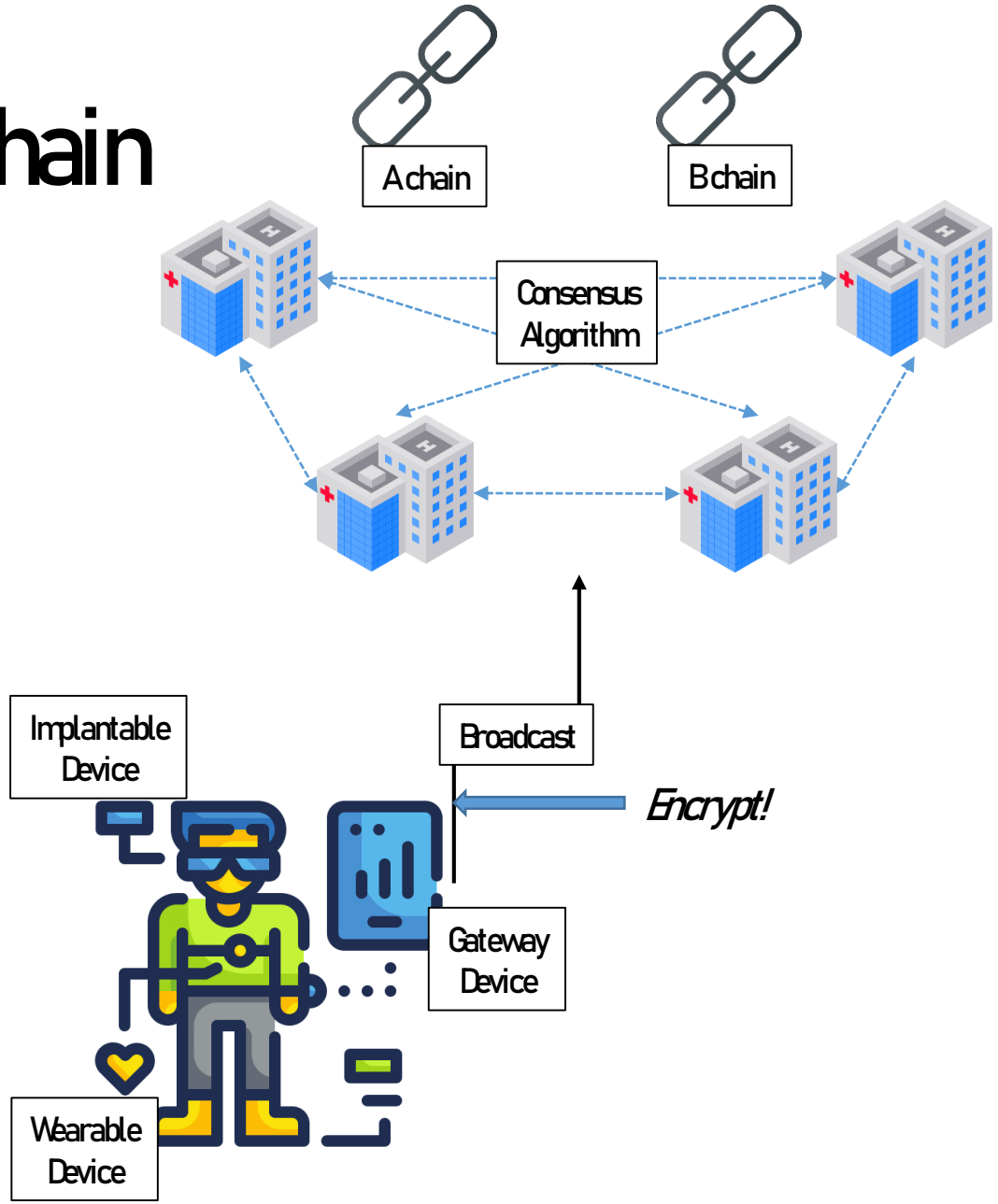
Original BSNs Problems

- Monopoly Problem
- Vulnerability Problem
- Privacy Problem
- Integrity Problem

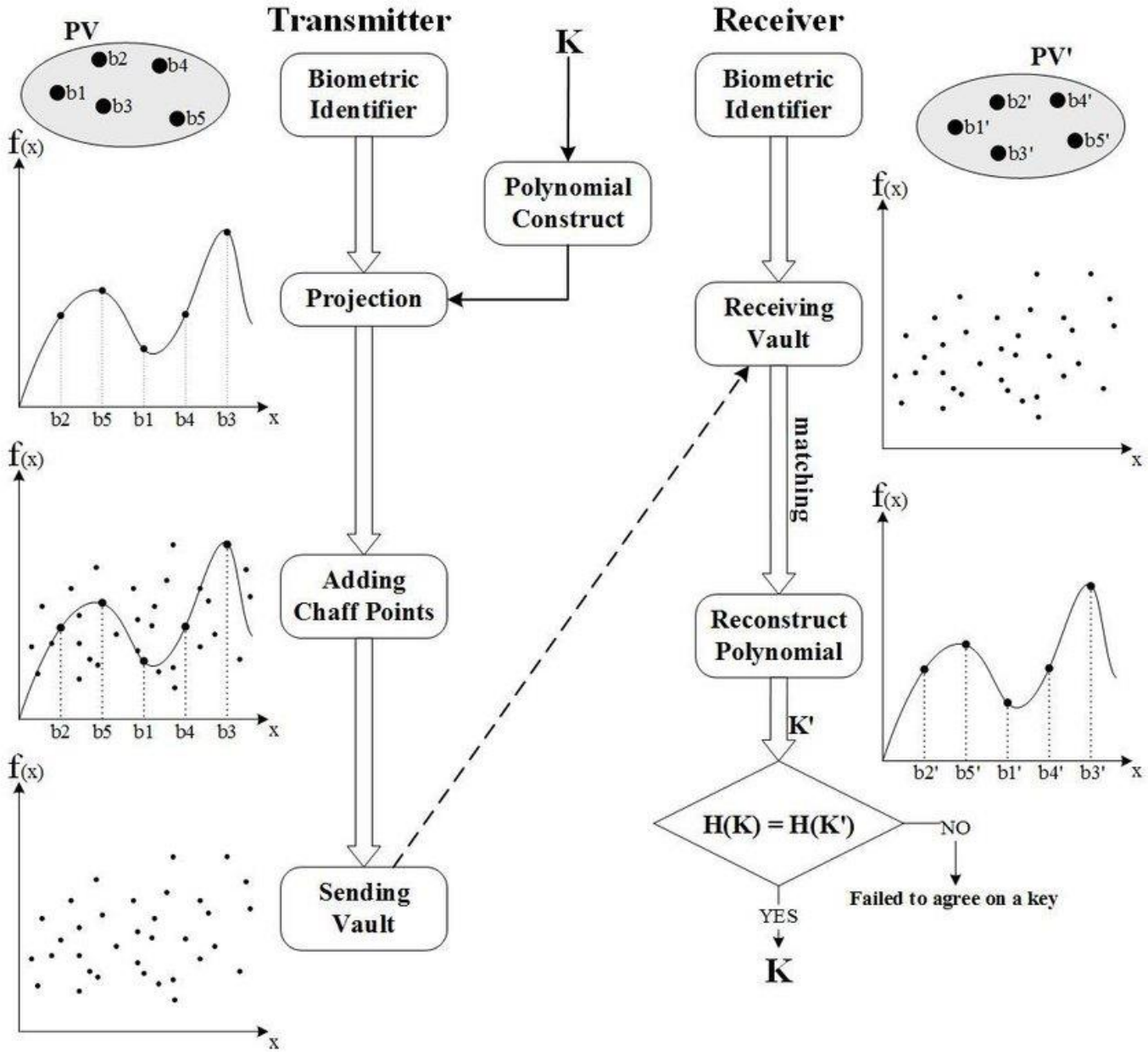


Proposed BSN using Blockchain

- Monopoly Problem
- Vulnerability Problem
- Privacy Problem
- Integrity Problem



Fuzzy Vault


Transmitter
Receiver
PV
PV'
K
Biometric Identifier
Biometric Identifier
Polynomial Construct
Projection
Receiving Vault
Adding Chaff Points
Reconstruct Polynomial
matching
K'
Sending Vault
H(K) = H(K')
NO
Failed to agree on a key
YES
K
f(x)
x
b1
b2
b3
b4
b5
b1'
b2'
b3'
b4'
b5'

Fuzzy Vault using PPG (photoplethysmography) signal

I. Production of PPG vector.
   I. Collect PPG signals
   II. Encoding signals into vectors using FFT (fast Fourier transform)

$$F_s =< f_s^1, f_s^2, \dots, f_s^a >, F_r =< f_r^1, f_r^2, \dots, f_r^a >$$

II. Creating Polynomial.
   I. Create $p(x)$ with a public order a
   II. Coefficients are produced from a random number → common key

$$Coef. = e_a, e_{a-1}, \dots, e_1, e_0 , Key = e_a \parallel e_{a-1} \parallel, \dots, \parallel e_1 \parallel e_0$$

Fuzzy Vault using PPG (photoplethysmography) signal

III. Vault Production.

I. Compute a set $D = \{f_s^i, p(f_s^i)\}, 1 \leq i \leq a$

II. Build a chaff points set $C = \{c_i, d_i\}, 1 \leq i \leq W$ using random numbers $d_i \neq p(c_i)$ (predefined)

III. Vault $R = D \cup C$

IV. Vault Transmission.

I. Send $R \parallel T(K, R)\ where\ T\ is\ MAC\ function$

V. Opening Vault.

I. Reconstruct $p(x)\ using\ f_r^i$, Lagrangian Interpolation

II. Recovery K'

III. Validate K' using T

Fuzzy Vault using PPG signal problem

- $v + 1$ feature points for vth-order polynomial
- Relation between parameters
- Revised.
  - Key encoding
  - LOTR (Lower-order twice reconstruction)

Proposed BSN again

I. Initialization period
    I. Some biosensor can generate key
    II. Set specific node A
II. When gateway device needs to encrypt
    I. Gateway gives order and asks A to generate key
    II. A makes pre-key $k_a \parallel k_{a-1} \parallel, \ldots, \parallel k_1, \parallel k_0$ and encodes it into codeword e_i
    III. A uses e_i as a coefficients to construct $\mathrm{ath} - \mathrm{order}\, p(x)$

Proposed BSN again

III. Making Vault
   I. A collects PPG signals from adjacent nodes.
   II. A encodes these signals into a vector F_s using FFT
   III. A makes vault $R = D \cup C$

IV. Encrypting Vault

   I. A calculates $K^* = F(k^*, \mathrm{K})$ as the encryption key
   II. A generates random number r
   III. Do $M = E(r \oplus k^*, R)$

Proposed BSN again

V. Sending to G
    I. A sends $K^* \parallel M \parallel r \parallel H(K^*) \parallel ID_A$ to Gateway device G
VI. Broadcasting
    I. G uses K^* to encrypt physiological data Mp
    II. G broadcasts $e(Mp)$ and $M \parallel r \parallel \mathrm{H}(\mathrm{K}^*) \parallel ID_A \parallel B_A$
    III. G deletes the K^*

Proposed BSN again (Recovering) $e(Mp)$ and $M \parallel r \parallel \mathrm{H}(\mathrm{K}^*) \parallel ID_A \parallel B_A$

I. Searching block
   I. User uses gateway to point out block on chain
   II. G searches block by index B_A
   III. G sends $M \parallel \mathrm{r} \parallel H(K^*)$ to A

II. Once A received
   I. Decrypt M using r, k^* to get vault R
   II. Collect signals from adjacent biosensors
   III. Encoding these signals and recovery $p(x)$ using LOTR and interpolation

III. Verifying
   I. A decodes coefficients from $p(x)$ using RS code
   II. A checks $H(K^*) = H(K^{*'})$

Security and performance analysis

I. Attacking the blockchain

$e(Mp)$ and $M \| r \| \mathrm{H}(\mathrm{K}^*) \| ID_A \| B_A$

$R = D \cup C$

II. Attacking the BSN
   I. On or into the human body
   II. Increase order

III. Performance
   I. BSN nodes are in charge of generation, backup, recovery