Breizh C@mp
Mix de technologies

CRYPTOGRAPHY, the swiss army knife of secured APIs

#BzhCmpCrypto

Sébastien Lambour - @FinistSeb

Too long title

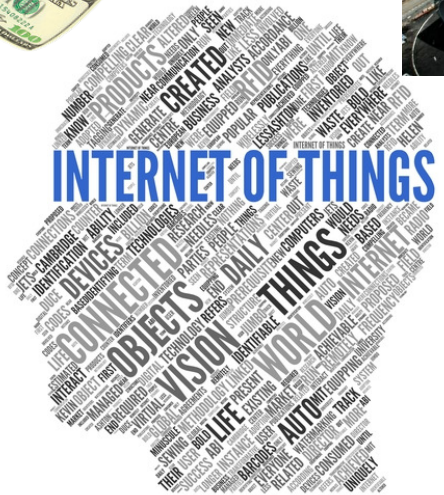
Who am I

Cityzen Data

BREST TECH

La FRENCH TECH

Authorization & Authentication



FDJ

Inspired from a true story

#LOYALTY

#TRANSFERT

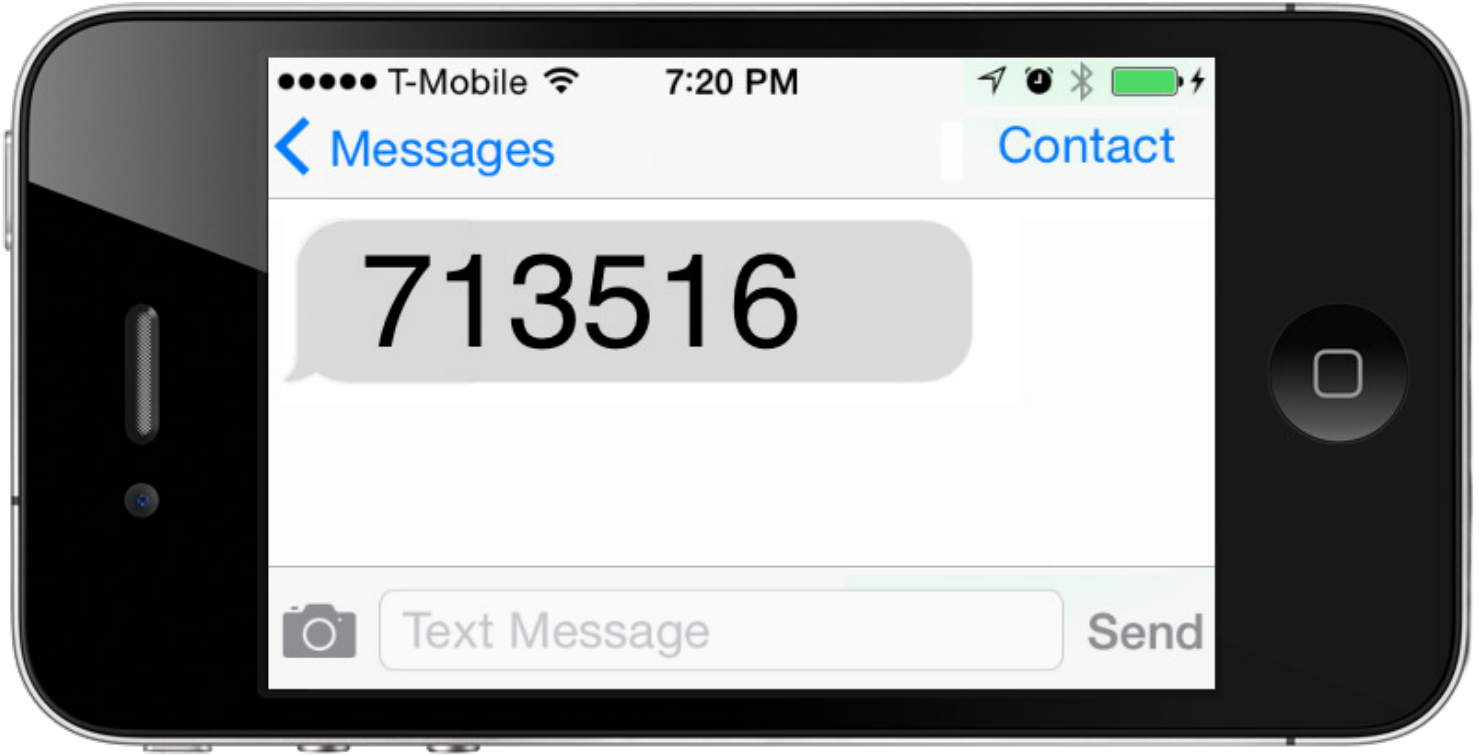
Banque JARAF (J’en ai rien à foutre)

Alice to Bob

FROM :	XXXFR-55555-1234567890-42
TO :	XXXJA-12125-6662391327-69
AMOUNT :	100 €

Are you sure?

I’m serious… no?



I looooooove HTTP post

POST / HTTP/1.1
content-type:application/x-www-form-urlencoded;charset=utf-8
host: https://raraf.bank
content-length:207
from=XXXFR-55555-1234567890-42
&to=XXXRU-22222-ANOTHER222-11
&amount=1000
&otp=713516


WE DID IT!!!
TROLL ME

Banque Back To The Future

Alice to Bob

FROM :	XXXFR-55555-1234567890-42
TO :	XXXJA-12125-6662391327-69
AMOUNT :	100 €

Seems not to bad...

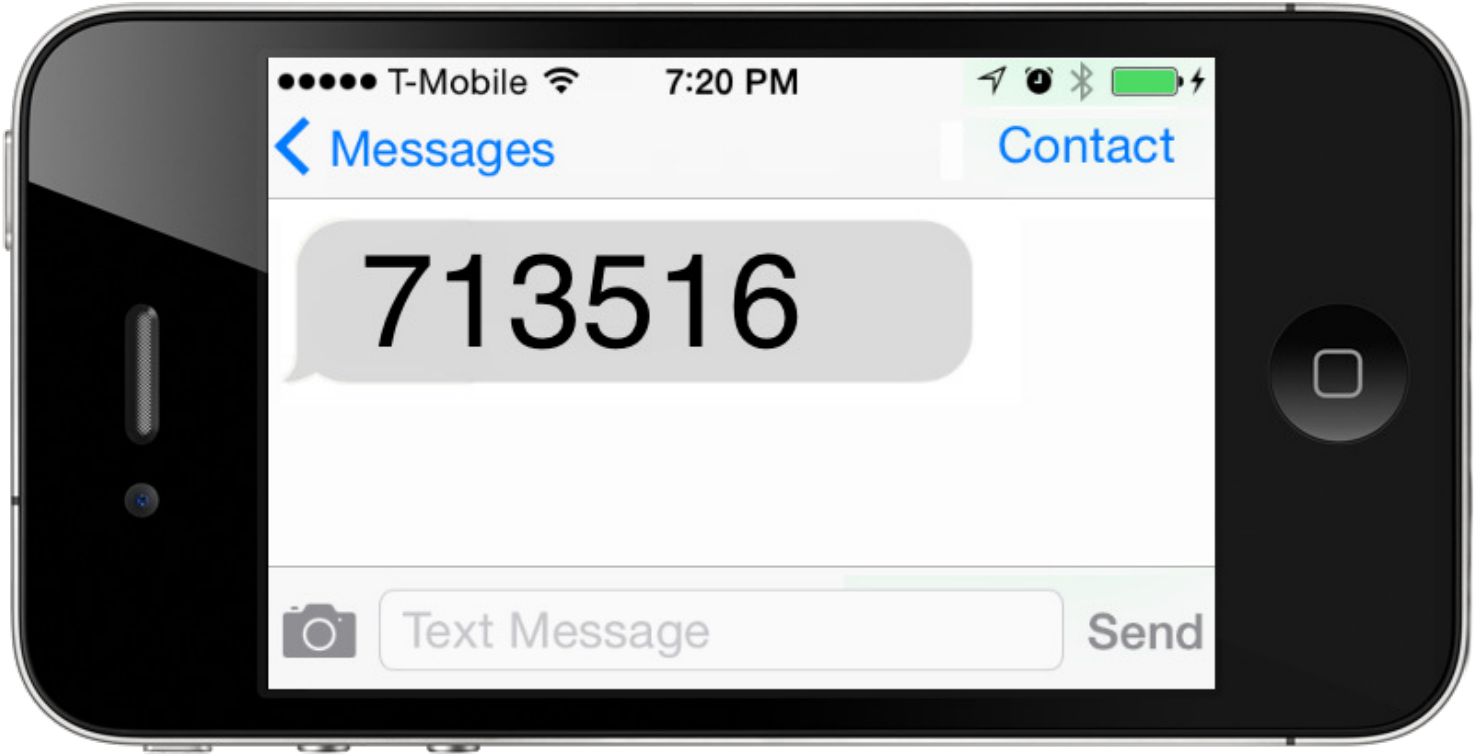
AUTHORISATION CODE : C6D8DF8E6A347473

Are you sure?

I looooooove HTTP post

POST / HTTP/1.1
content-type:application/x-www-form-urlencoded;charset=utf-8
host: https://backtothefuture.bank
content-length:207
from=XXXFR-55555-1234567890-42
&to=XXXJA-12125-6662391327-69
&amount=100
&auth_code=C6D8DF8E6A347800

I’m serious… no ?



I looooooove HTTP post

POST / HTTP/1.1
content-type:application/x-www-form-urlencoded;charset=utf-8
host: https://backtothefuture.bank
content-length:207
&otp=713516
&auth_code=C6D8DF8E6A347800

Seems serious… or not

Coincidence ?

AUTHORISATION CODE : C6D8DF8E6A347800
AUTHORISATION CODE : C6D8E76316324800

Too simple...

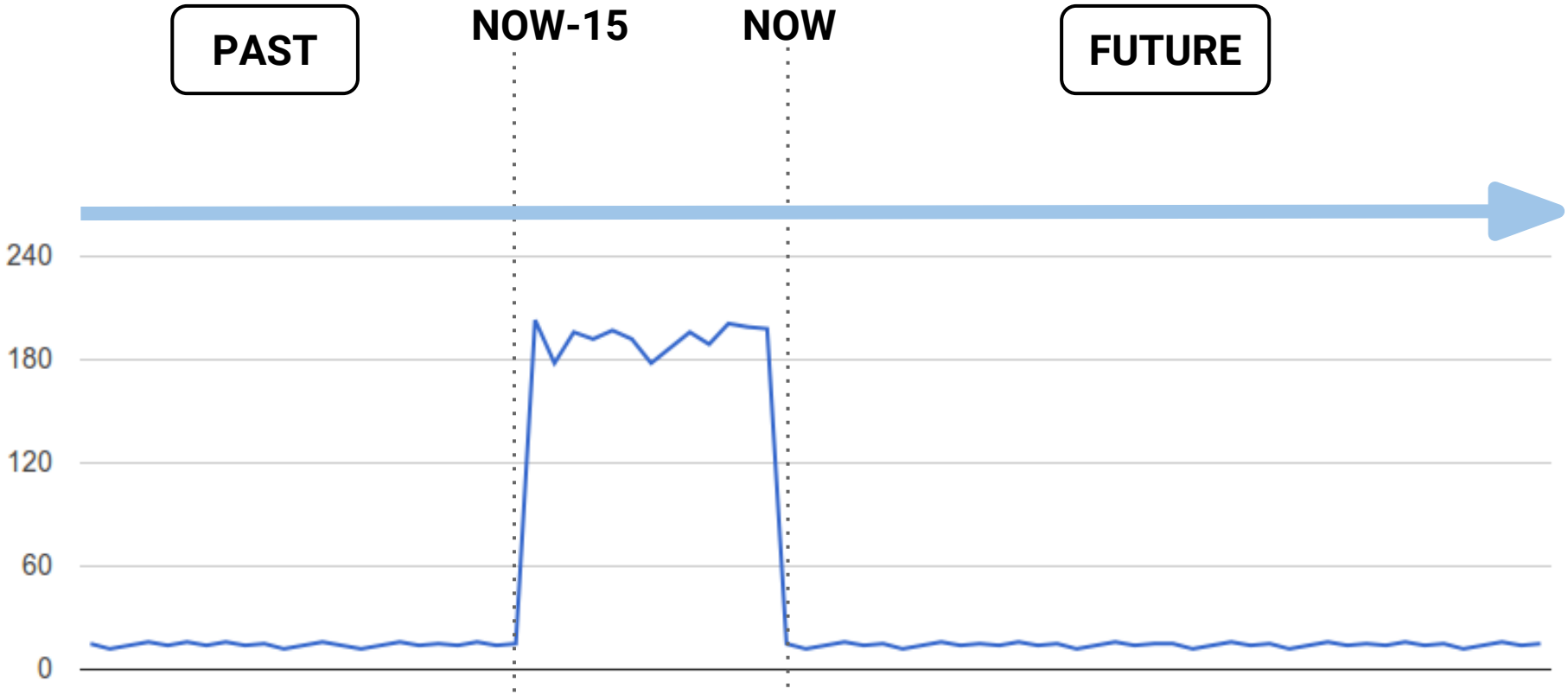
28/5/2015 à 22:26:41

C6D8DF8CBABA14B3 -> 1432844801**0000405683**
C6D8E76166B7E8C5 -> 1432845662**0000405701**

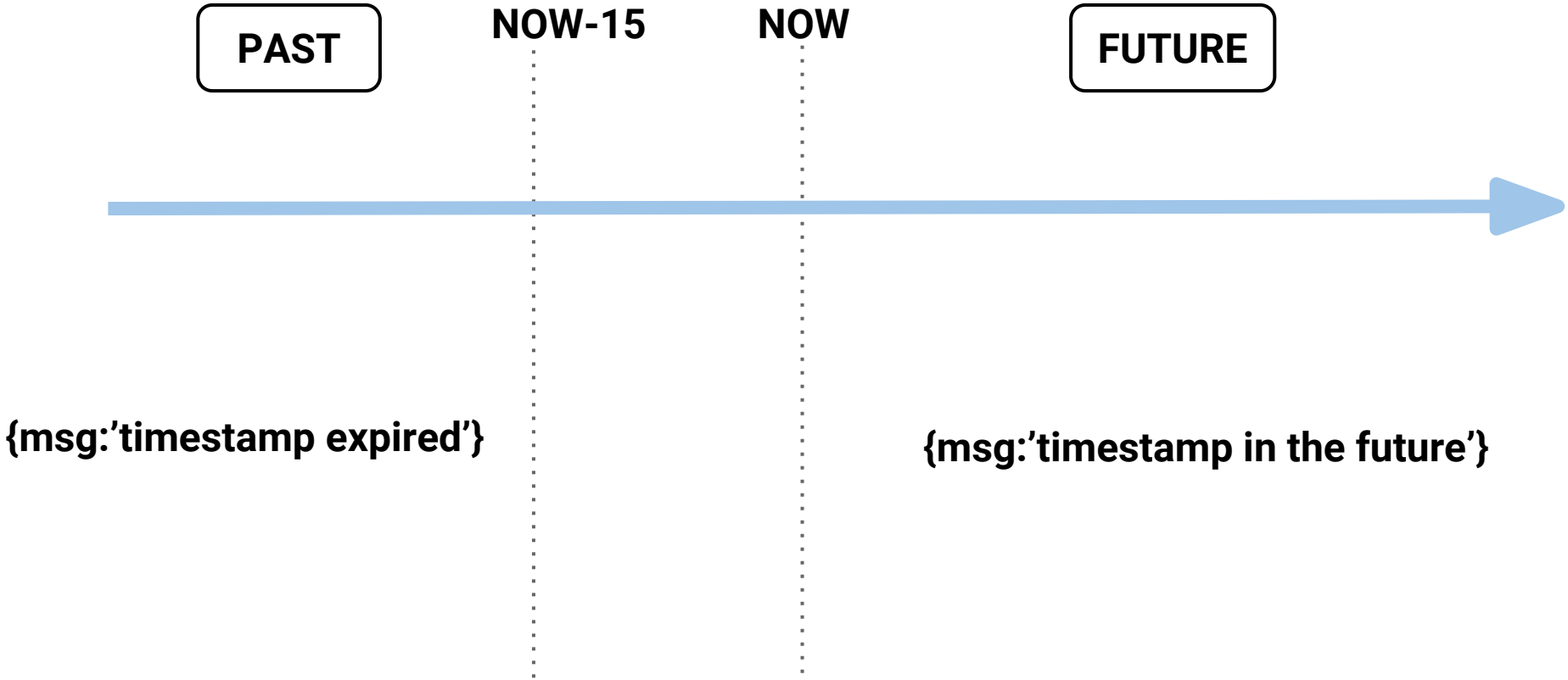
28/5/2015 à 22:41:02

SHALL WE PLAY A GAME?

Play with timestamp



Verbose API


PAST
NOW-15
NOW
FUTURE
{msg:'timestamp expired'}
{msg:'timestamp in the future'}

Very verbose API

NOW-15

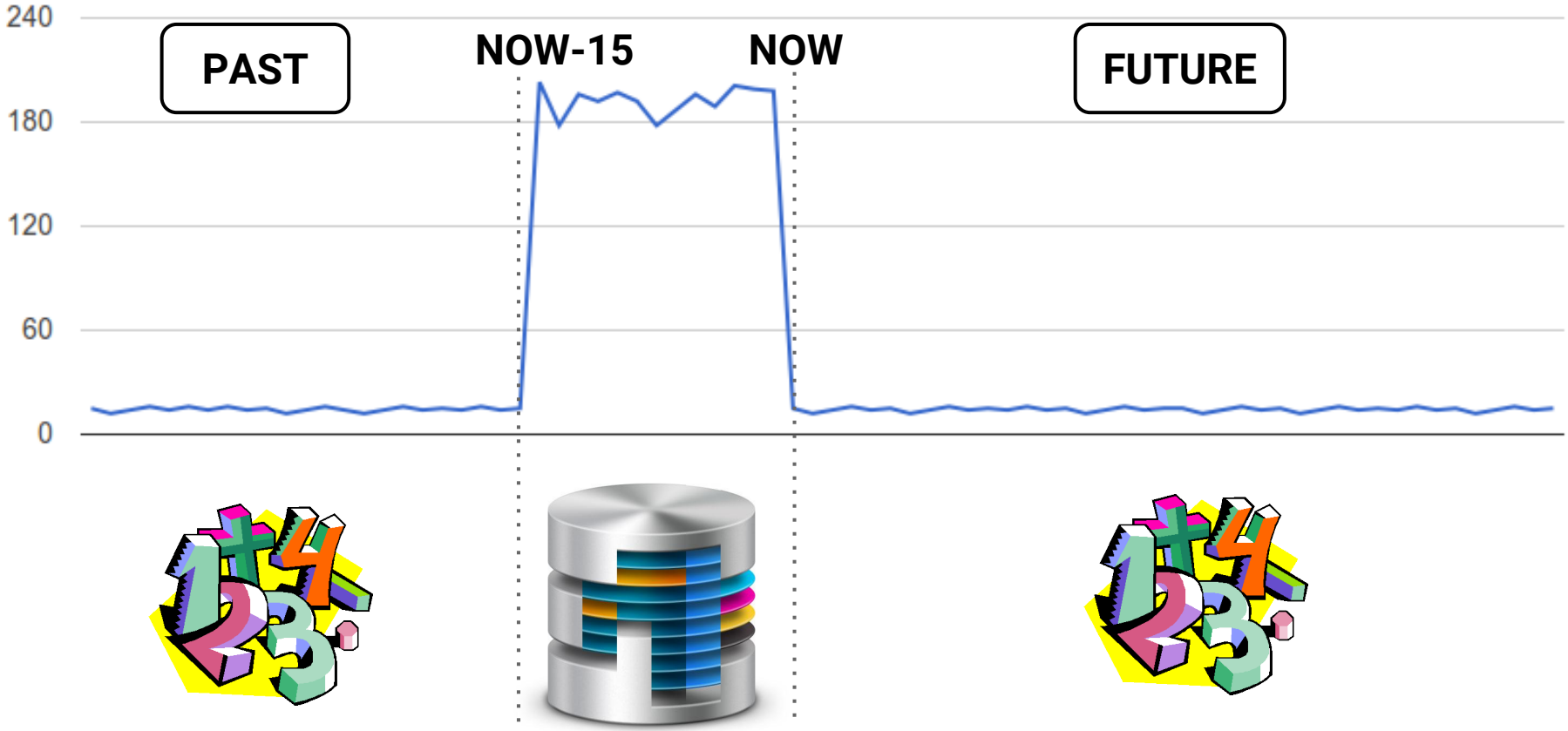
NOW

{msg:’sequence unknown’}

{msg:’sequence already validated’}

{msg:’bad user’}

Play with timestamp




Le thème c'est "Bounty Hunter",
"chasseur de prime" en anglais, pas Bounty.
LegoJeff

#PROBLEM


GRAILS

...

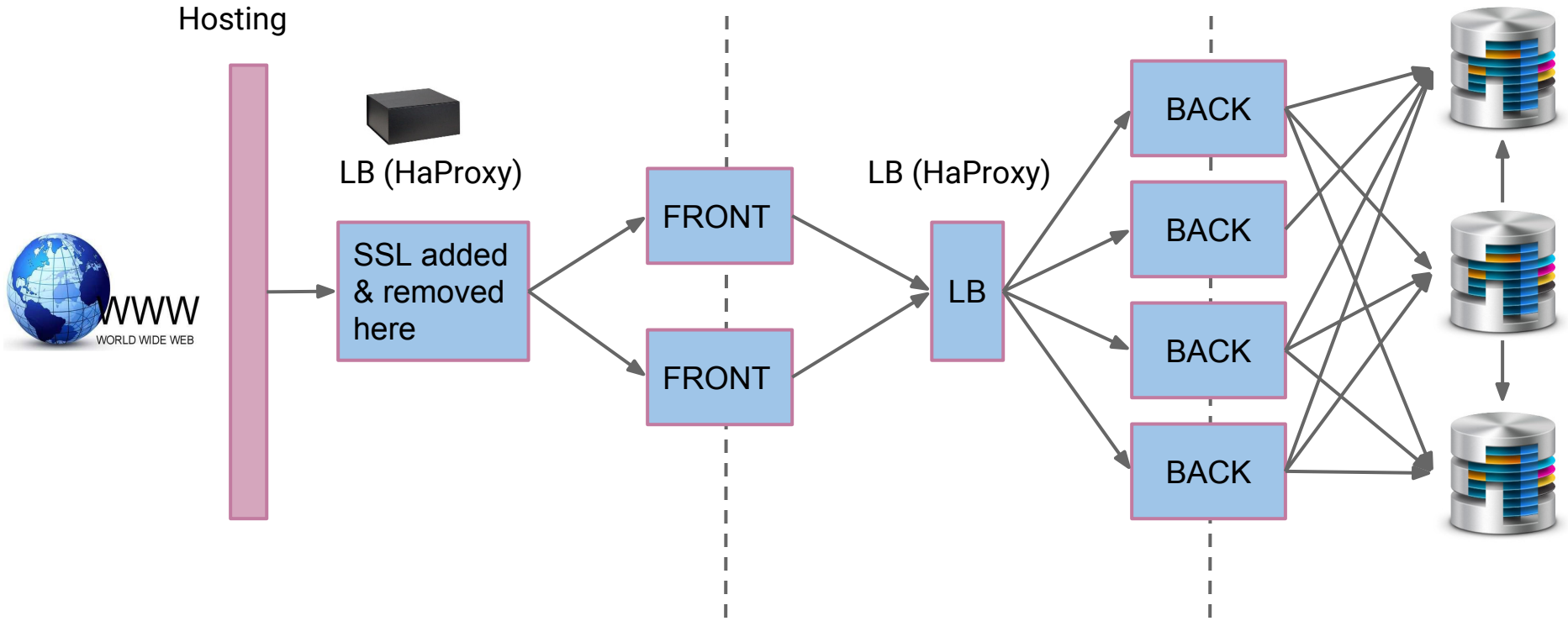
#STATE

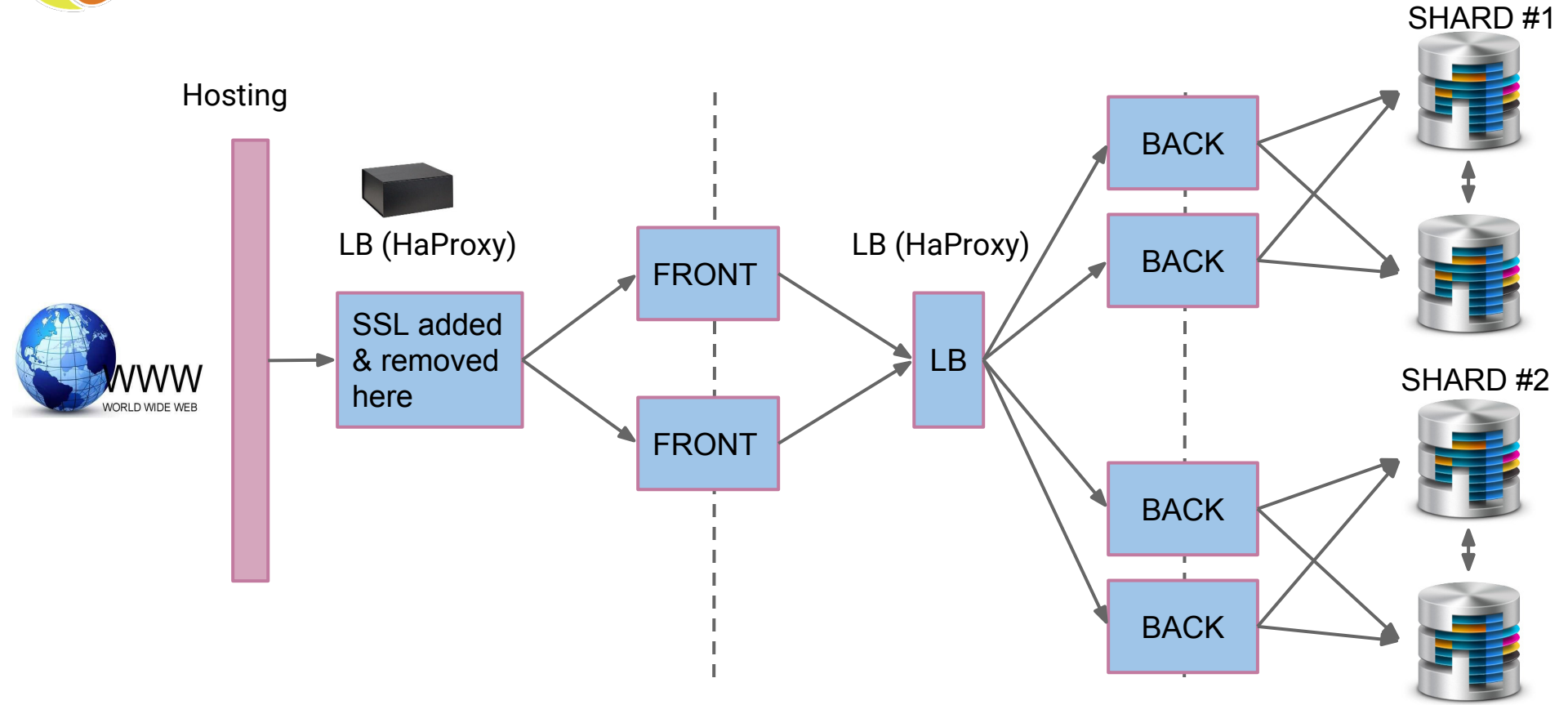
37%	XSS
16%	SQL Injection
5%	Path disclosure
4%	Denial of service attack
4%	Arbitrary code execution
4%	Memory corruption
3%	Cross-site request forgery
3%	Data breach
4%	File inclusion (Arbitrary, Local, Remote)
1%	Buffer overflow
15%	Other, including code injection (PHP/JS), etc

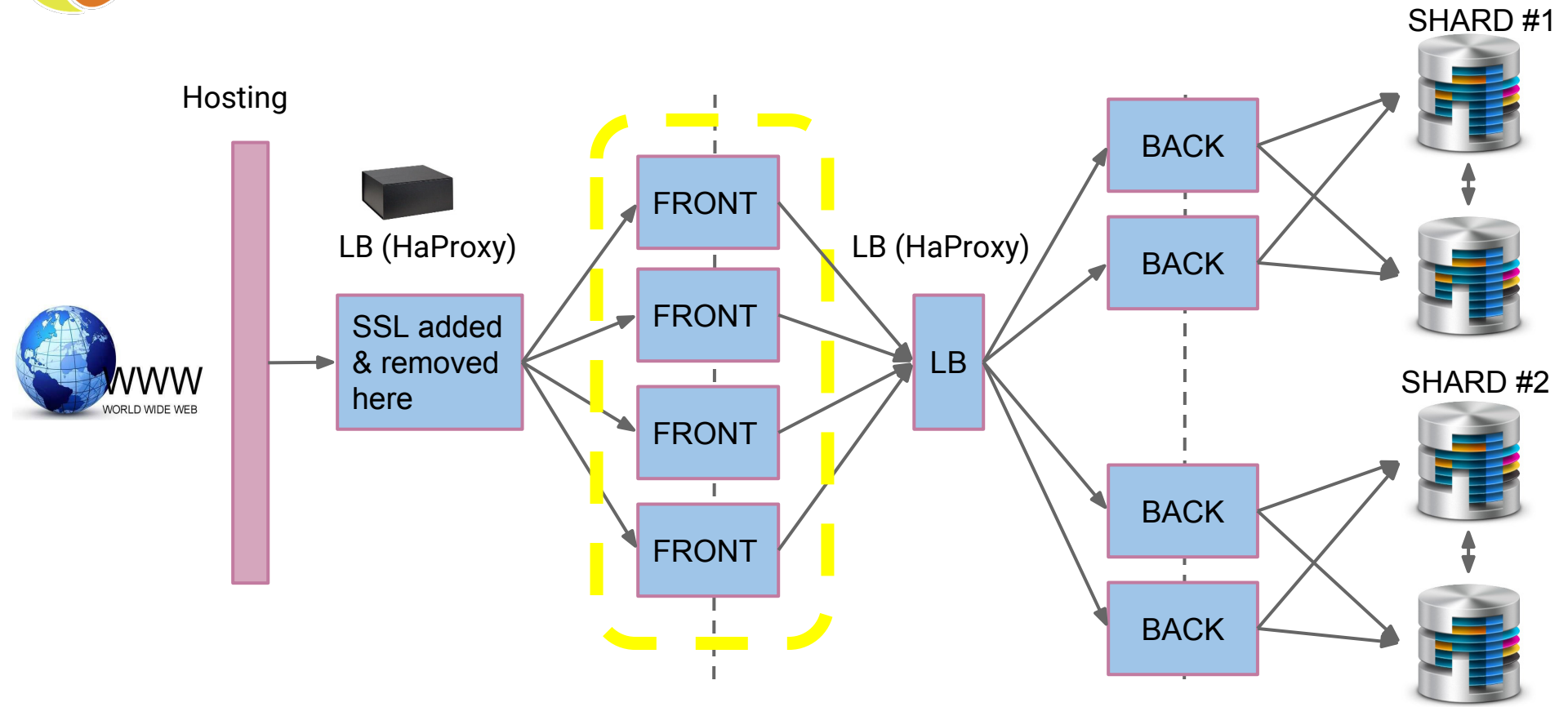
#1

#2 In the code (business)

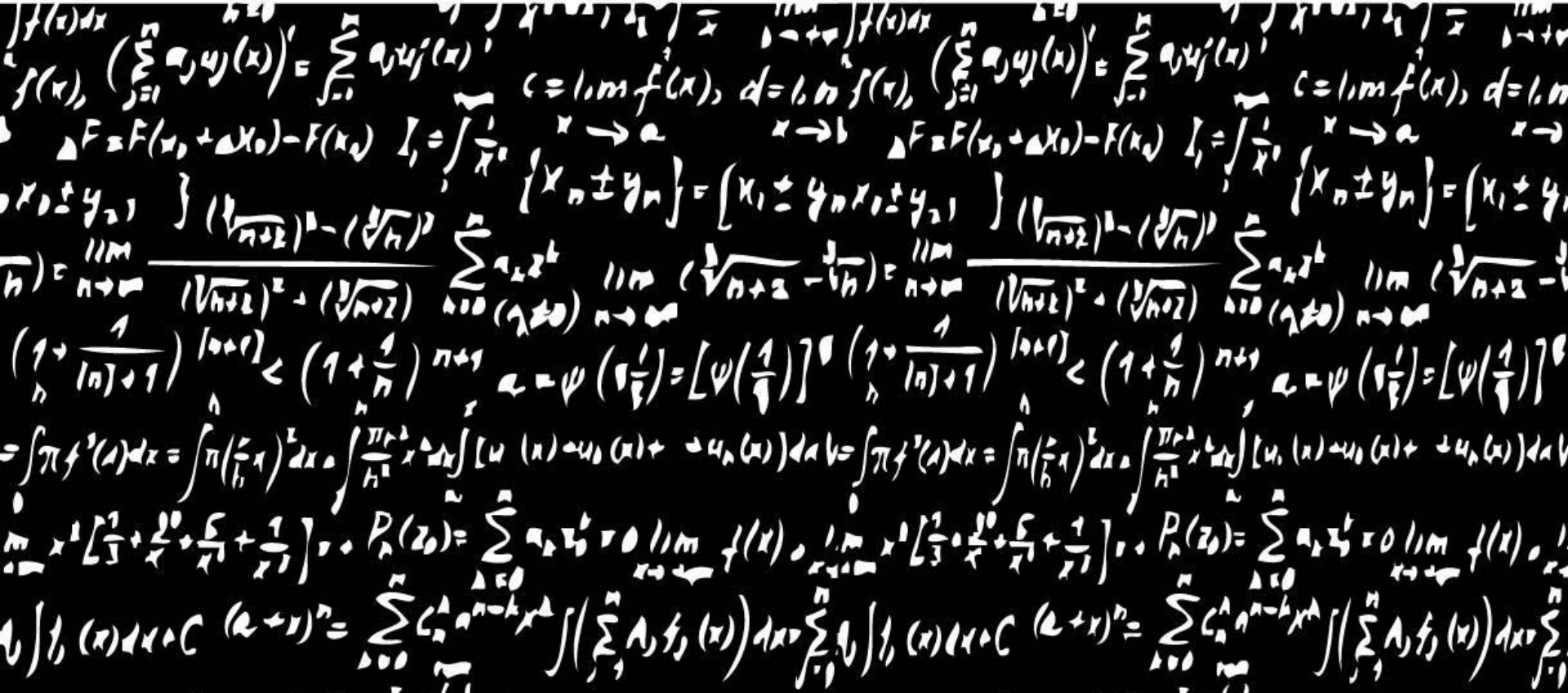
#3 SCALABILITY


Hosting
LB (HaProxy)
SSL added & removed here
FRONT
FRONT
LB (HaProxy)
LB
BACK
BACK
BACK
BACK
WWW
WORLD WIDE WEB


Hosting
LB (HaProxy)
SSL added & removed here
FRONT
FRONT
LB (HaProxy)
LB
BACK
BACK
BACK
BACK
SHARD #1
SHARD #2
WWW
WORLD WIDE WEB


Hosting
LB (HaProxy)
SSL added & removed here
WWW
WORLD WIDE WEB
FRONT
FRONT
FRONT
FRONT
LB (HaProxy)
LB
BACK
BACK
BACK
BACK
SHARD #1
SHARD #2

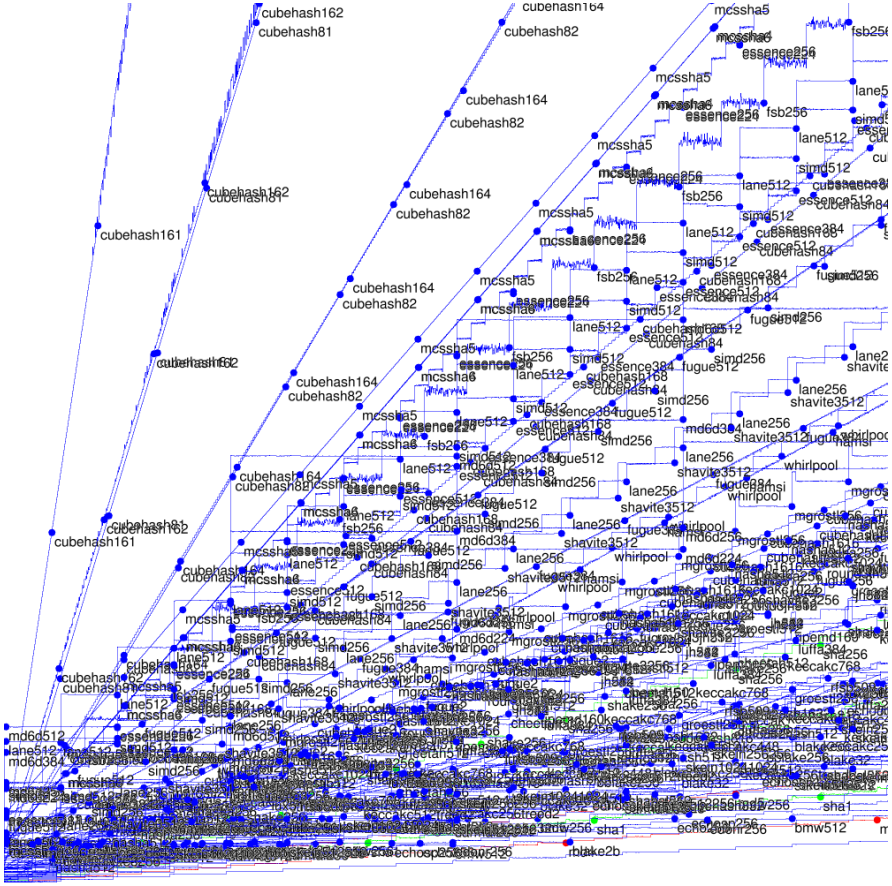
#Crypto can help you



#Crypto can help you

Symmetric cryptography

Cryptographic hash functions



Cryptographic hash functions

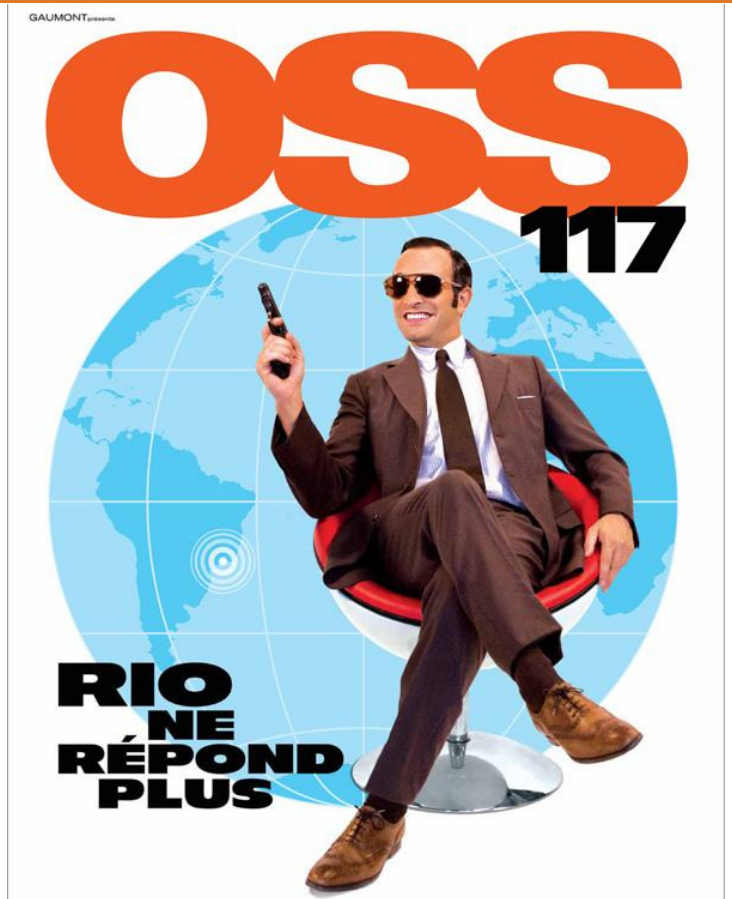
NEVER forget it

With Salting

Min salt size

Protect your keys

Open Secret Server



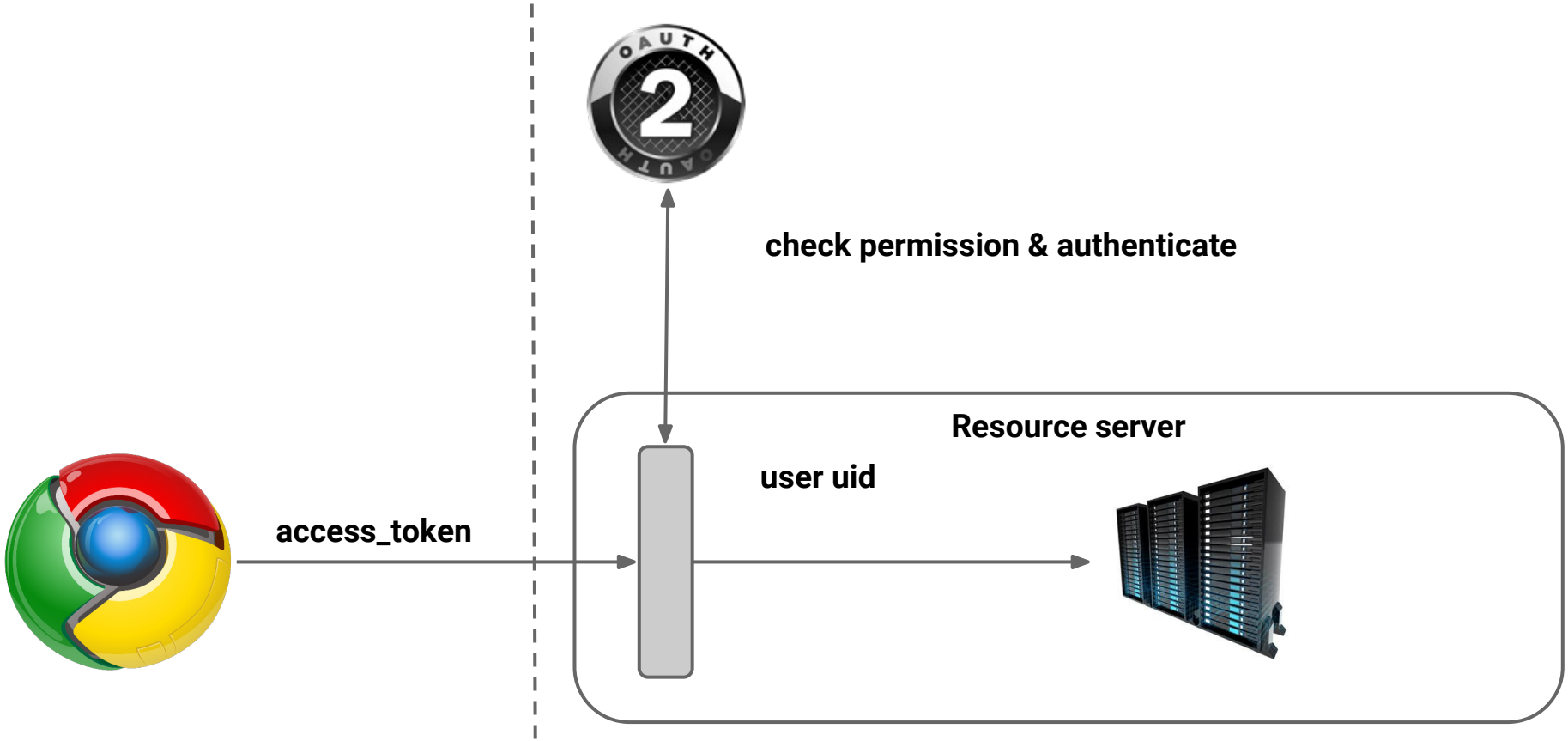
Shamir algorithm

#The limit...


BUSH, "WE DON'T TORTURE"
WE BAPTIZE!
By Riber Hansson, Svenska Dagbladet, Sweden

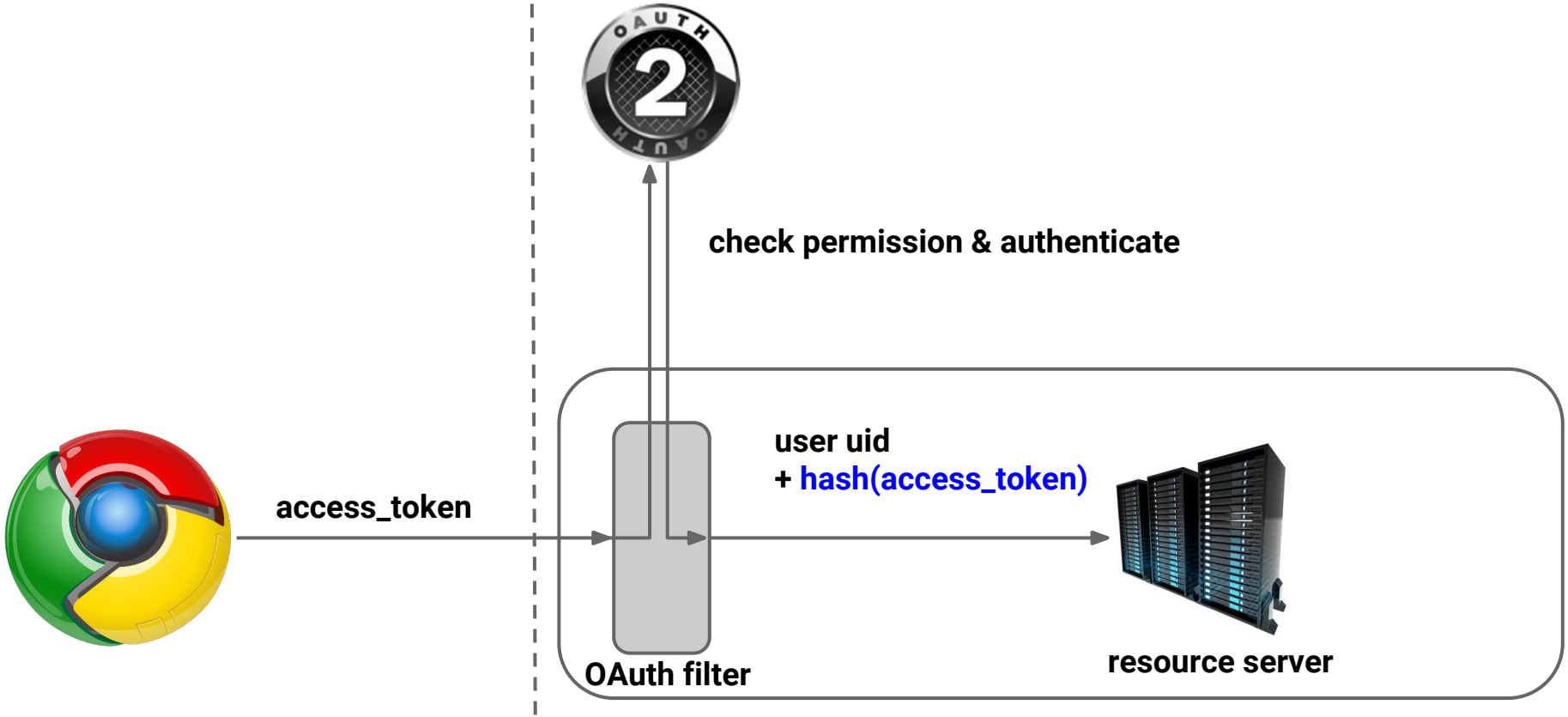

Go Ahead
It Will Be Fun

HTTP Request



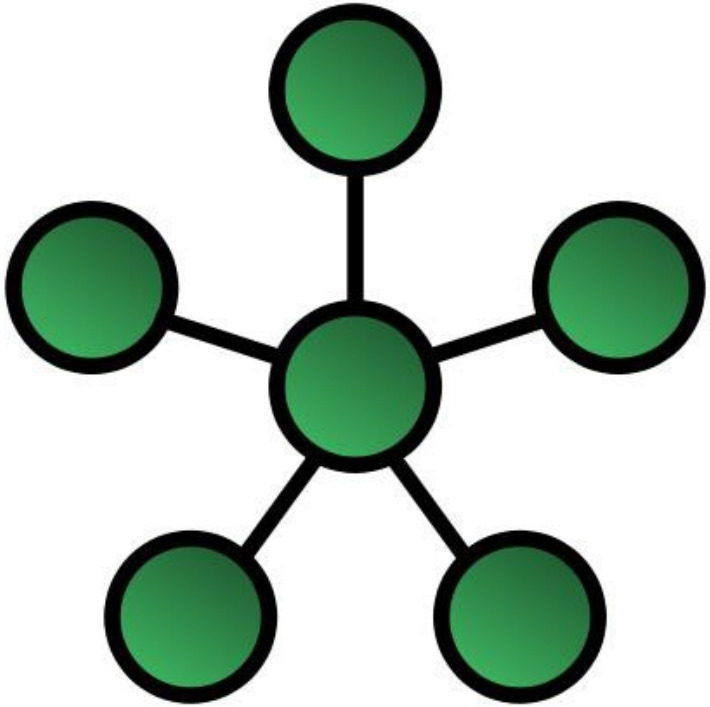

« Pas de bras, pas de chocolat... »
#INTOUCHABLES

HTTP Request



#TRANSFERT

Accounts availables



Accounts availables

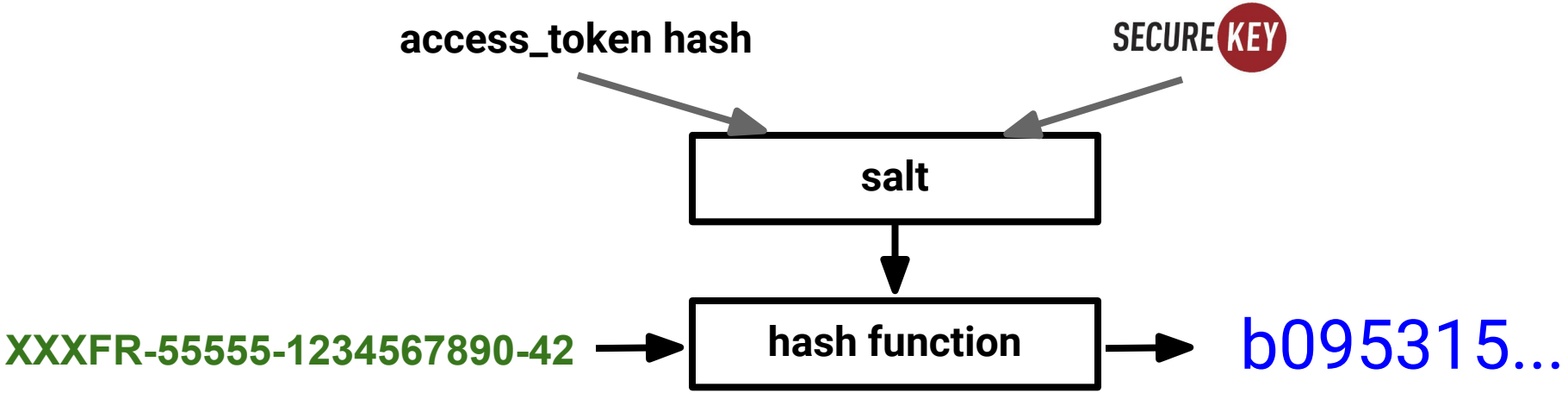
{

‘28b7b53...’:{... account description},

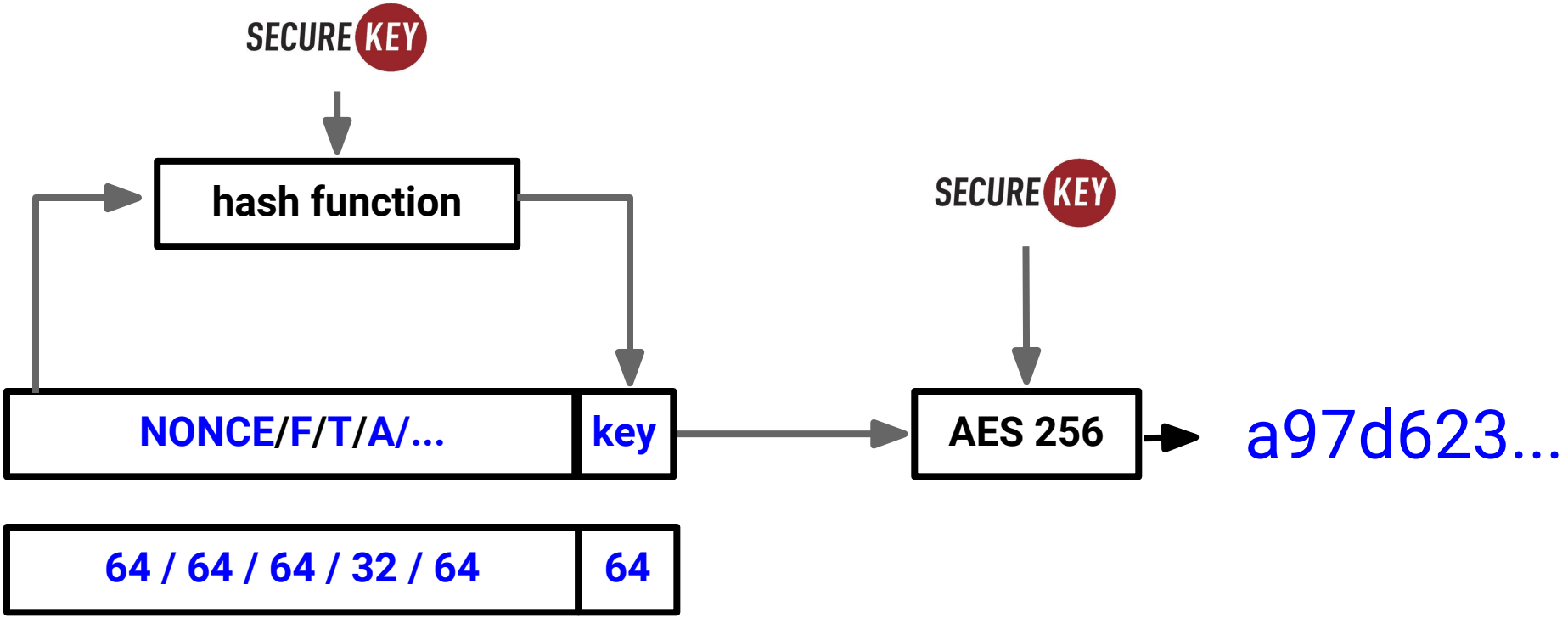
‘3bc118d...’:{... account description},

‘b095315...’:{... account description},

}


access_token hash
SECURE KEY
salt
XXXFR-55555-1234567890-42
hash function
b095315...

Authorisation code



Time machine (TOTP)

OTP (TOTP) with d digits

$$TC = (unixtime(now) - unixtime(T0)) / TS$$

$$TOTP = HOTP(\mathbf{SecretKey}, \mathbf{TC})$$

$$\mathbf{TOTP\text{-}Value} = TOTP \bmod 10^{d}$$

Compute the counter TC

```
byte[] text = new byte[8];
for (int i = text.length - 1; i >= 0; i--) {
        text[i] = (byte) (TC & 0xff);
        TC >>= 8;
 }
```

Hash Mac SHA1 OTP

```
public static byte[] hmac_sha1(byte[] keyBytes, byte[] text) throws...  {
        Mac hmacSha1 = Mac.getInstance("HMAC-SHA-1");

        SecretKeySpec macKey = new SecretKeySpec(keyBytes, "RAW");
        hmacSha1.init(macKey);
        return hmacSha1.doFinal(text);
}
```

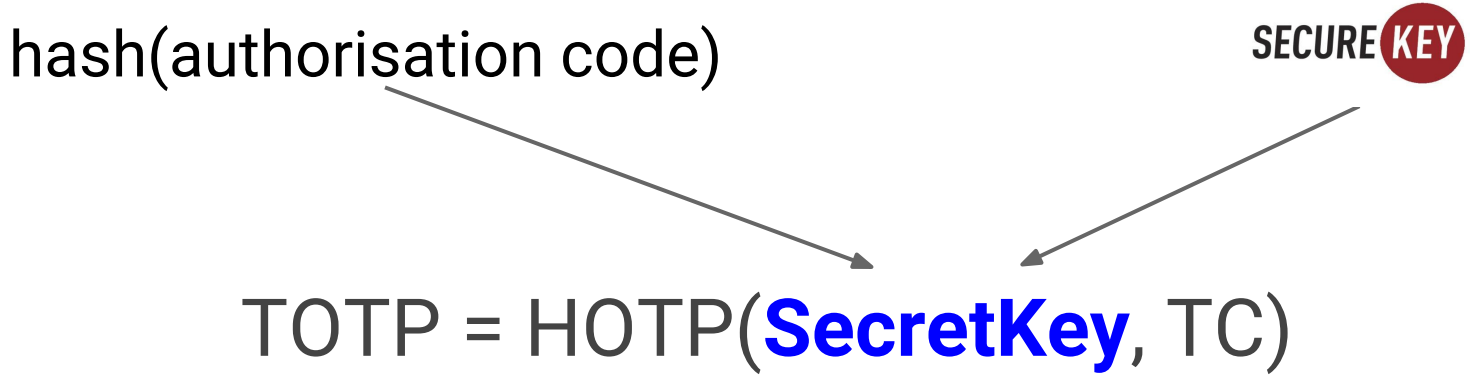
OTP (HOTP) with d digits

$$TC = (unixtime(now) - unixtime(T0)) / TS$$

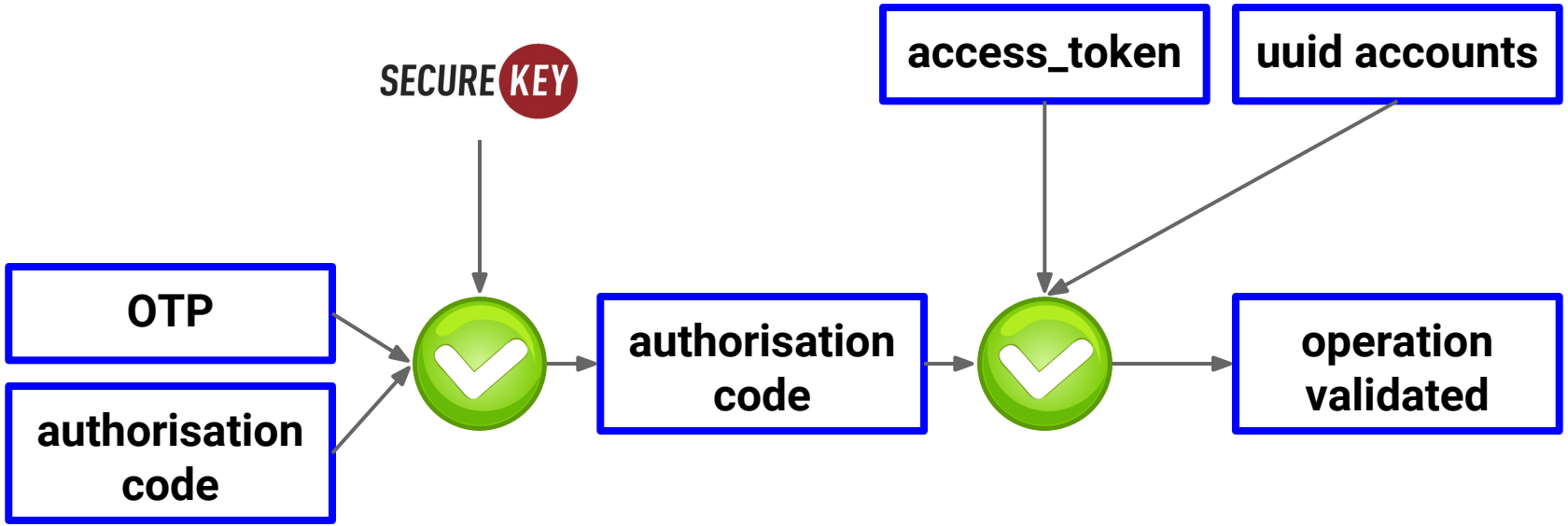
$$TOTP = HOTP(SecretKey, TC)$$

$$\textbf{TOTP-Value} = TOTP \bmod 10^{d}$$

OTP (TOTP)



Check transaction



Benefits

kill access_token and sleep deeply

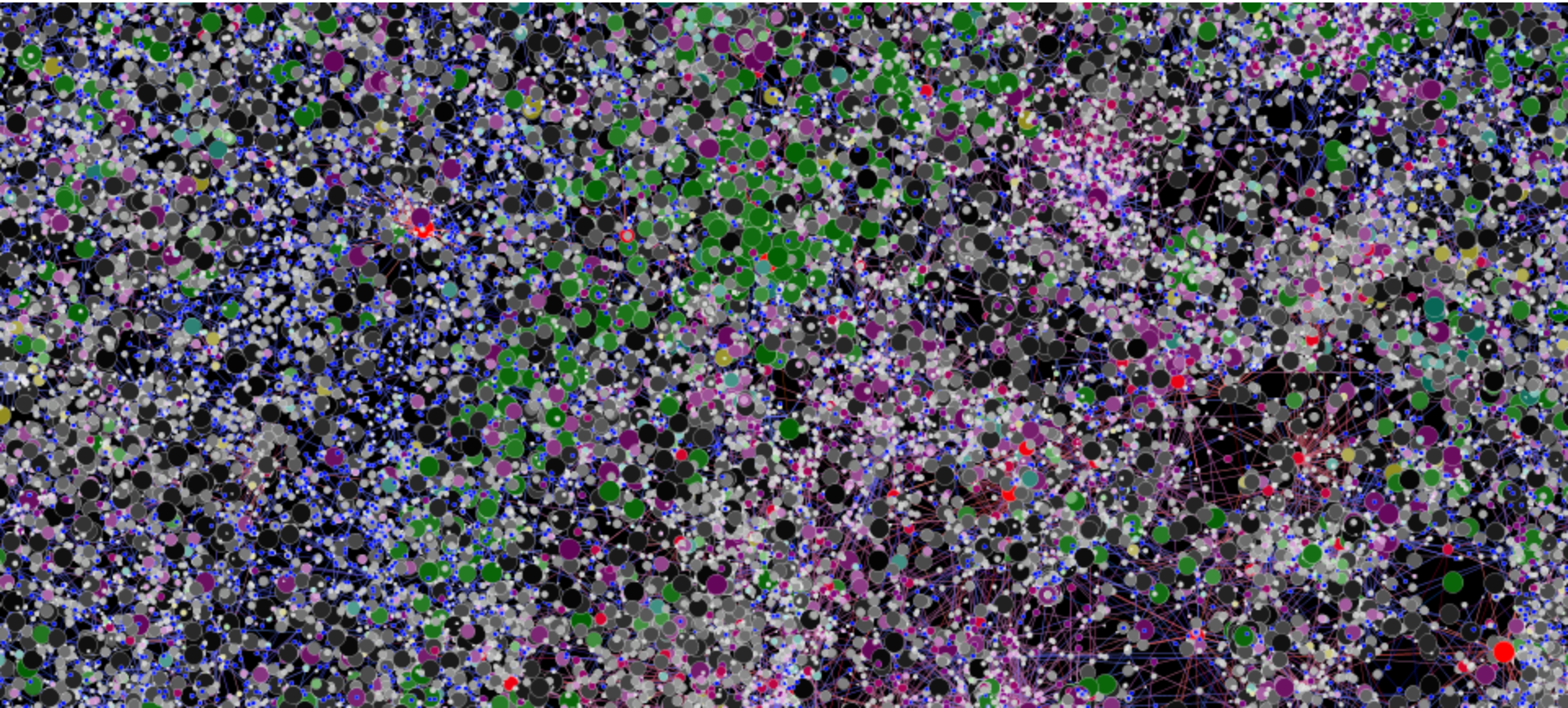
Benefits

Second factor is contextualized

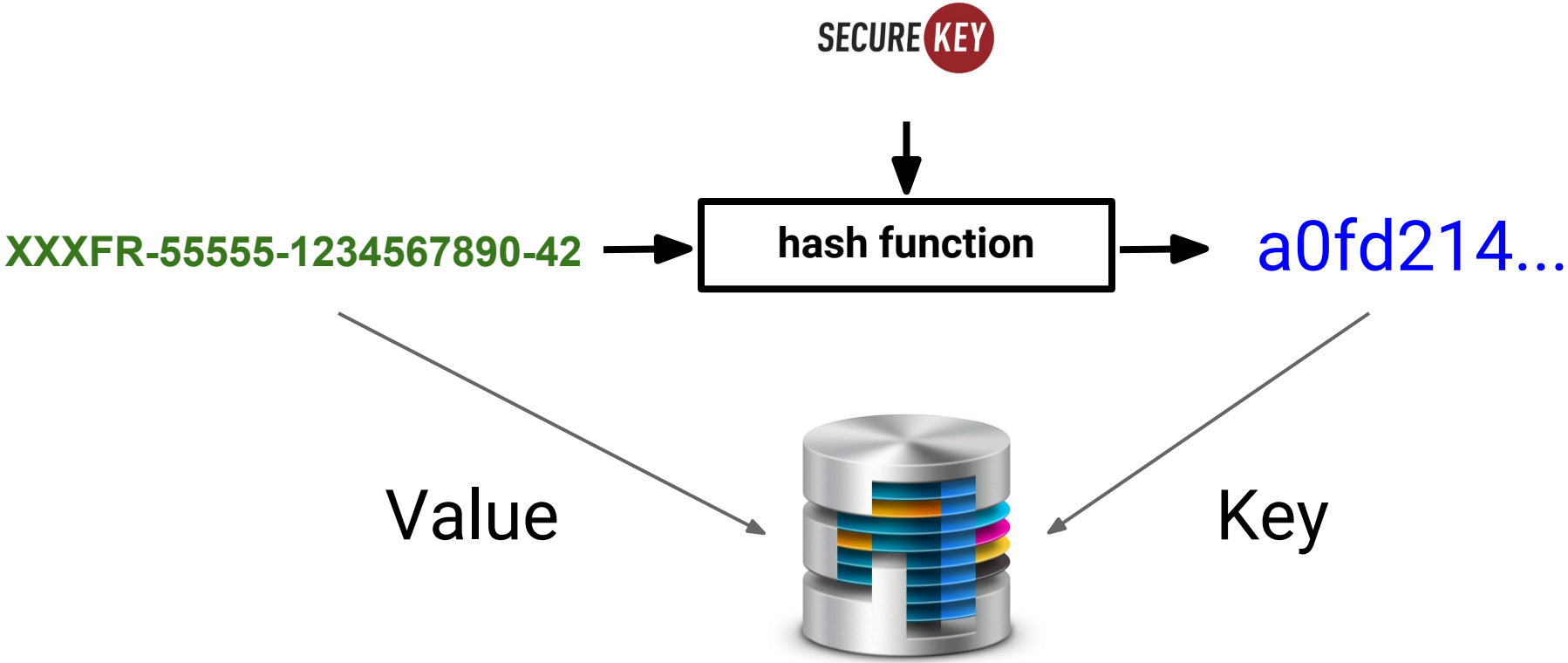
Limits: collated by computing

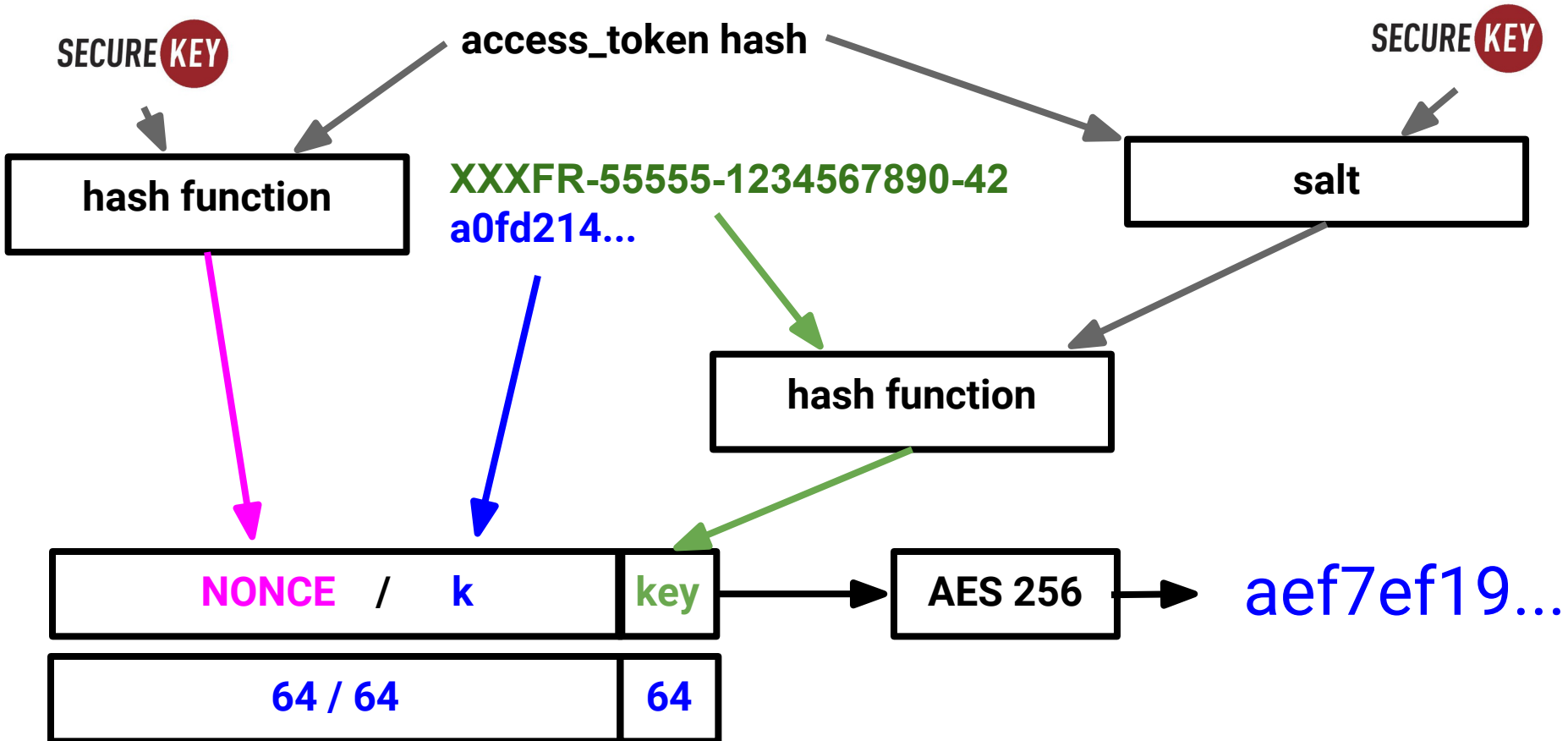
access_token hash	SECURE KEY	
XXXFR-55555-1234567890-42	**28b7b53** →	**28b7b53**
XXXJA-12125-6662391327-69	**3bc118d** →	**3bc118d**
XXXJA-12125-6662391328-54	b095315	100€
XXXJA-12125-6662391329-76 →	ef338a6	...
XXXJA-12125-6662391330-21	57a1d9f	
XXXJA-12125-6662391331-43	a8e2fc2	
XXXJA-12125-6662391332-19	43fc129	

large entries



k,v


SECURE KEY
XXXFR-55555-1234567890-42
hash function
a0fd214...
Value
Key


SECURE KEY
access_token hash
SECURE KEY
hash function
XXXFR-55555-1234567890-42
a0fd214...
salt
hash function
NONCE / k
key
AES 256
aef7ef19...
64 / 64
64

#Benefits

Immuable transaction per user

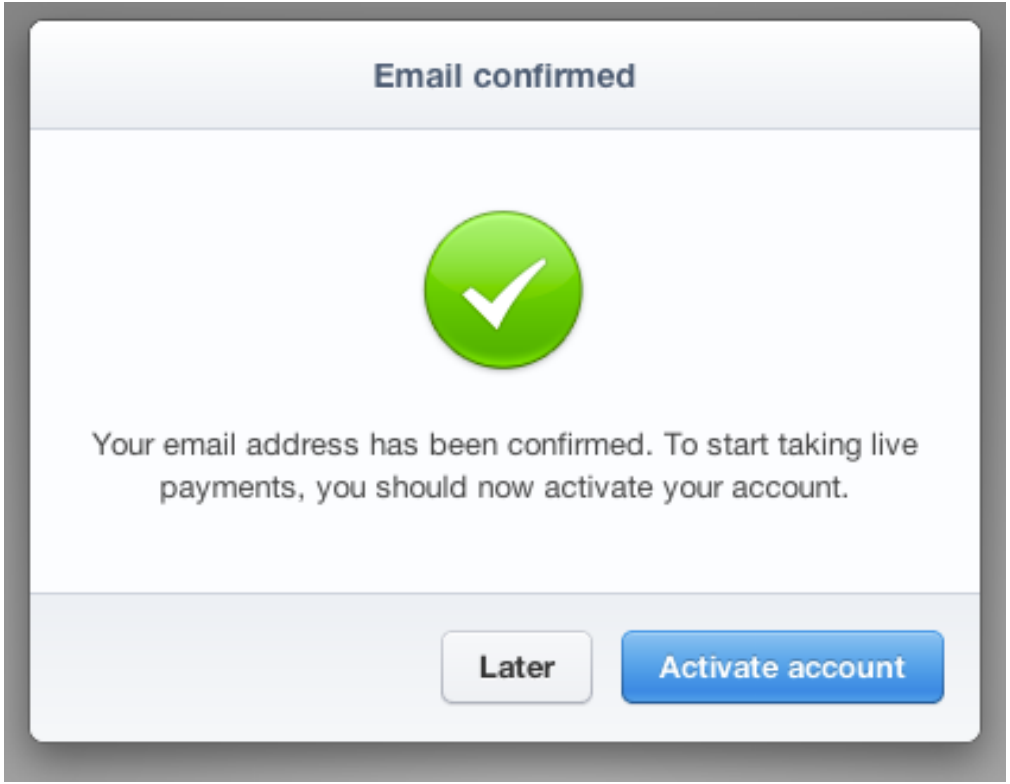
unreplayable

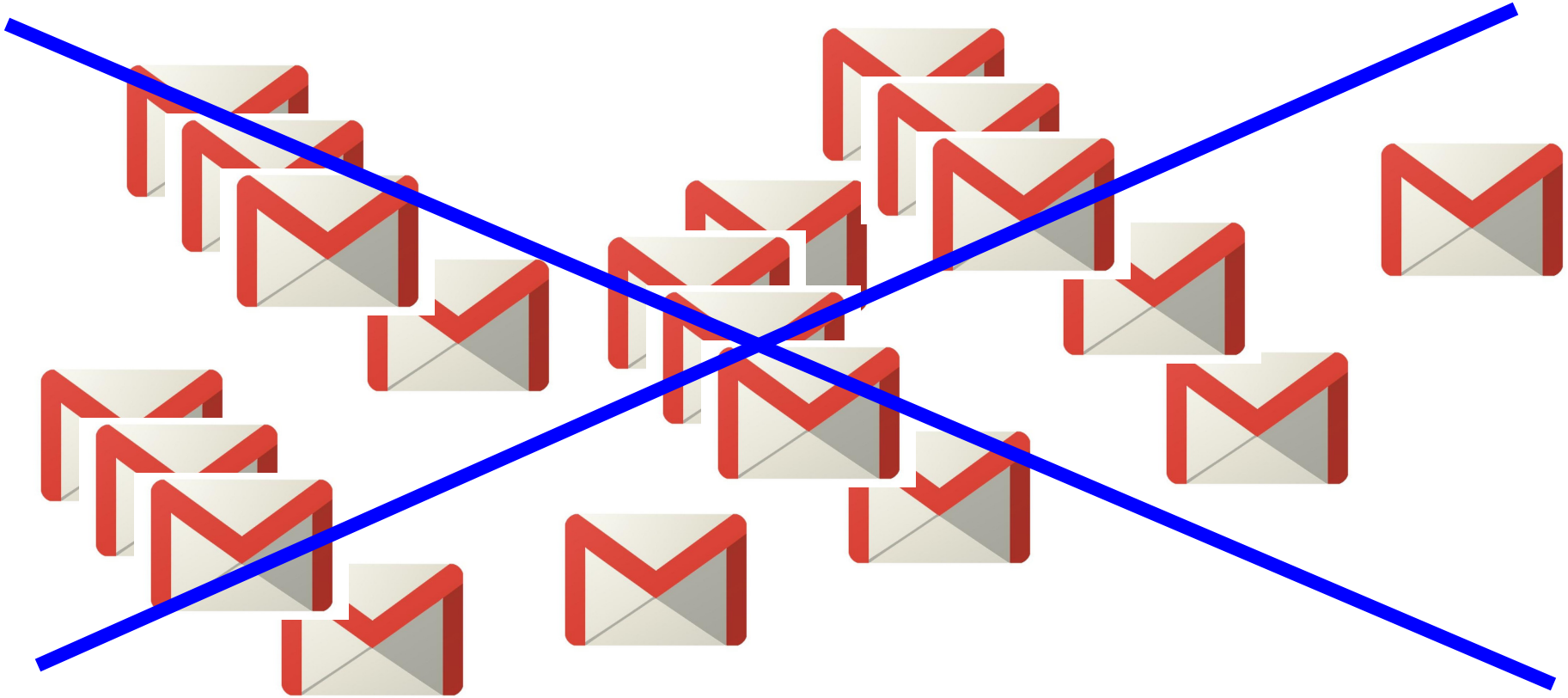
only legitim calls to backend

internal data structure not exposed


HARD BUT
GOOD


DANGER
HIGH VOLTAGE EQUIPMENT
AUTHORIZED
PERSONNEL ONLY
DANGER
HIGH VOLTAGE 90V
ELECTRIC SHOCK HAZARD
REMOVE POWER BEFORE
REPAIR OR ADJUSTMENT


Email confirmed
Your email address has been confirmed. To start taking live payments, you should now activate your account.
Later
Activate account



Email verification

Inbox x Notifications x

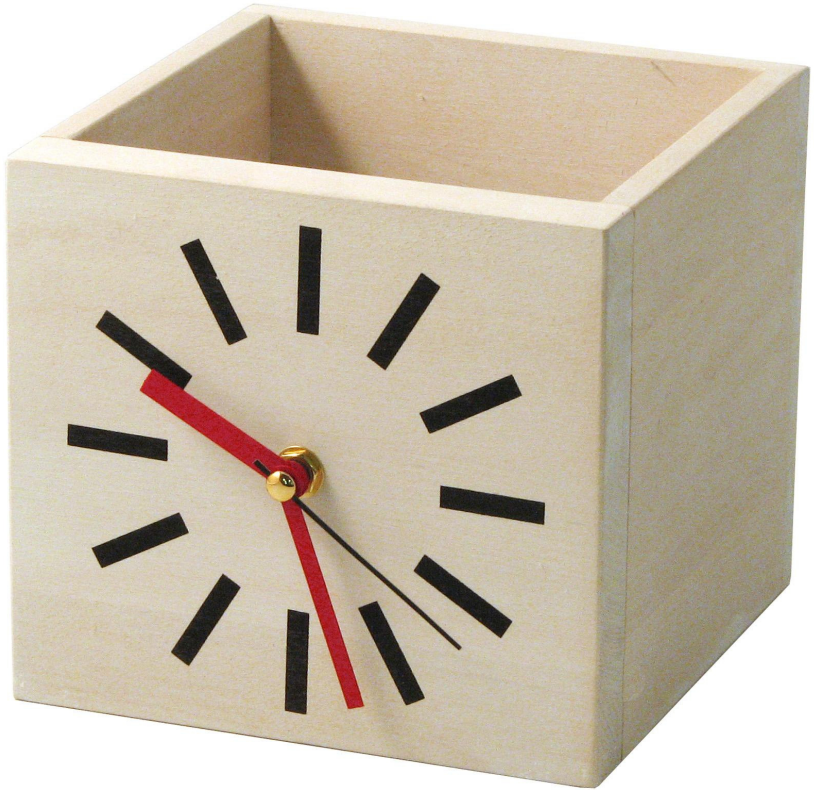
9lessons Demos labs@9lessons.info via ar 11:45 PM (59 minutes ago)

to me

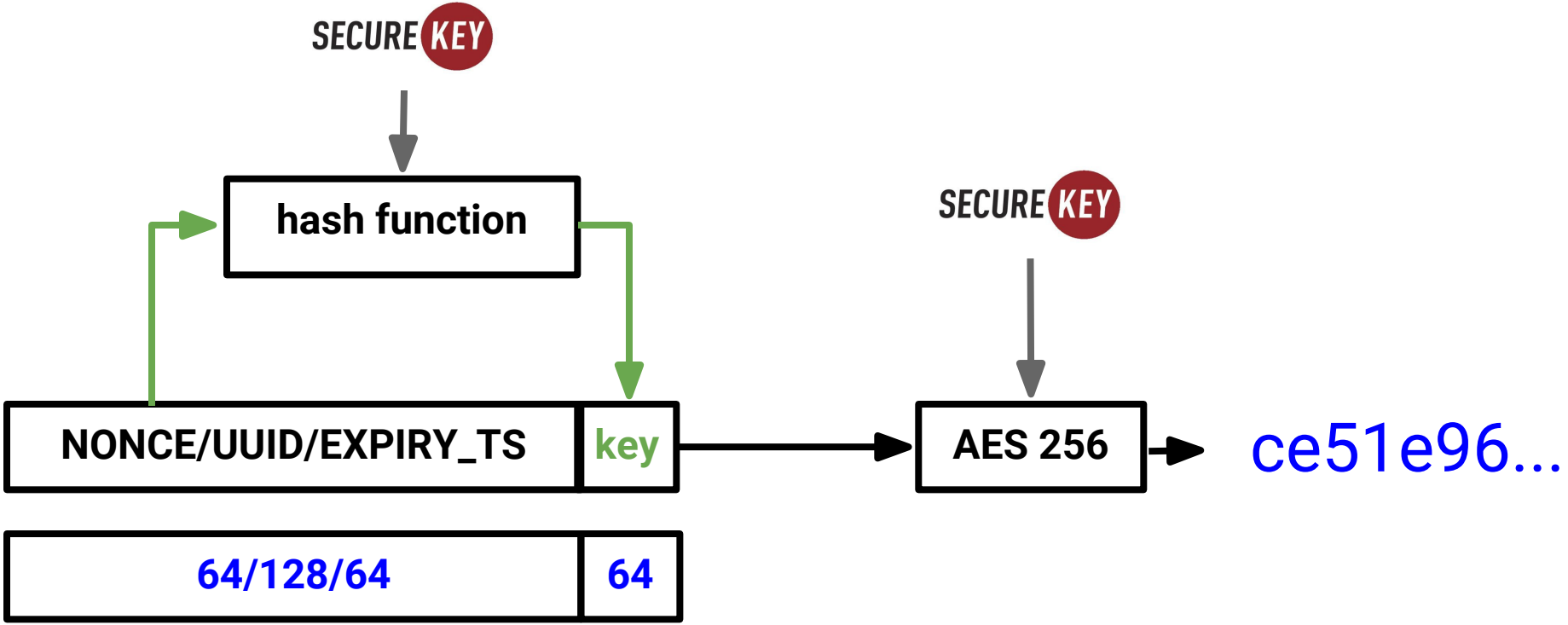
Hi,

We need to make sure you are human. Please verify your email and get started using your Website account.

http://demos.9lessons.info/email_activation/activation/3272f5b50d0c8ed0bb6361ca844f



Activation code



{

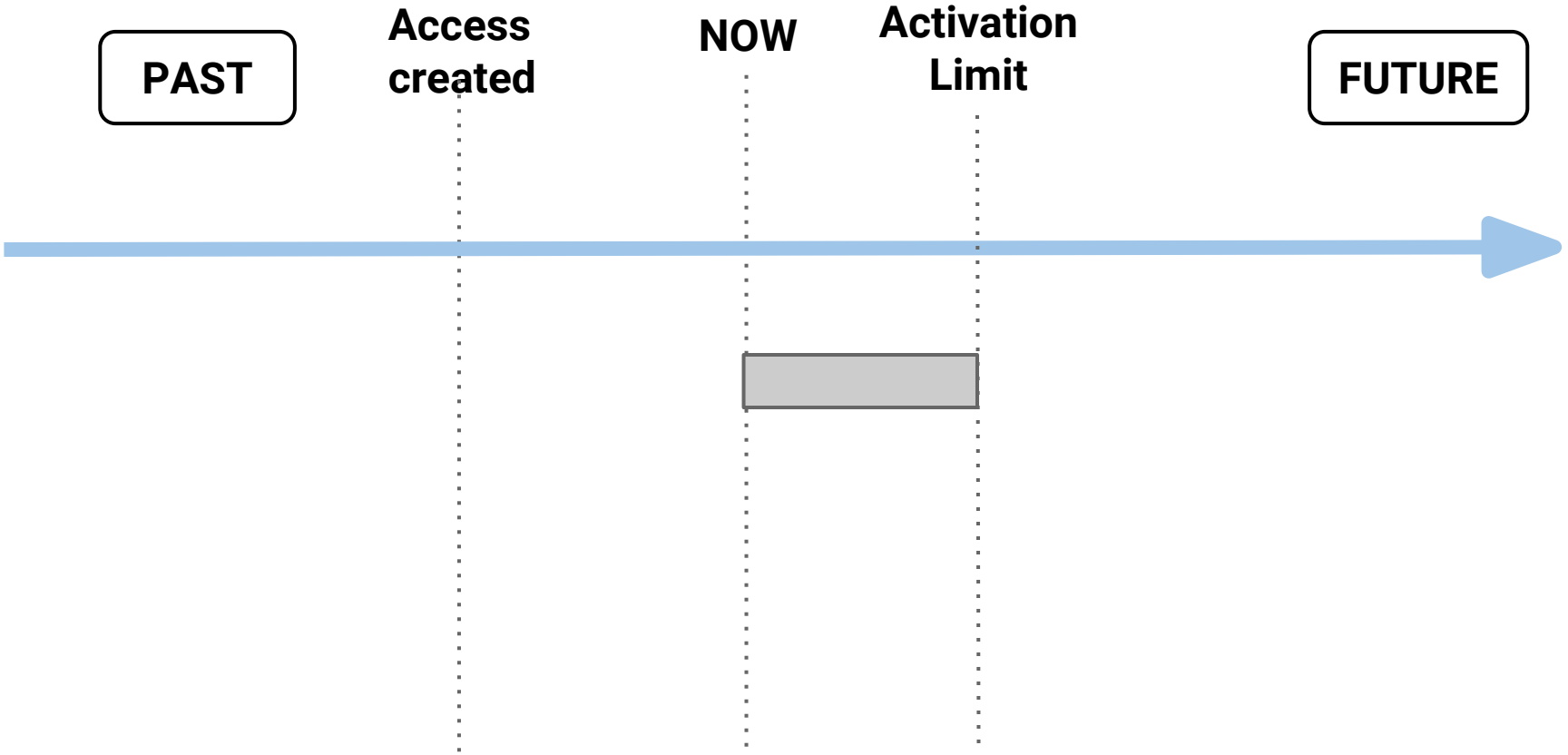
‘uuid’: ‘ca793aed-d653-4841-bb90-84e091acedaa’,

‘issuance’ : 1433600000000,

‘activation’: 1433683314198,

….

}


PAST
Access created
NOW
Activation Limit
FUTURE

Optimisation

hazelcast

KEY	ca793aed-d653-4841-bb90-84e091acedaa
VALUE	true
EXPIRY	timestamp expiry date

Encoding ?

Compare It

[63, -30, 44, -7, -34, -41, 74, 81]

3fe22cf9ded74a51

P+Is+d7XSlE=

#Problem

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghij
klmnopqrstuvwxyz0123456789**+/=**


60
55
5
50
10
45
15


We Can Code It!


ANY
QUESTIONS
?