HWallet
The simple cryptocurrency hardware wallet

HITBSecConf2018 - Dubai

Nemanja Nikodijević
<nemanja@hacke.rs>

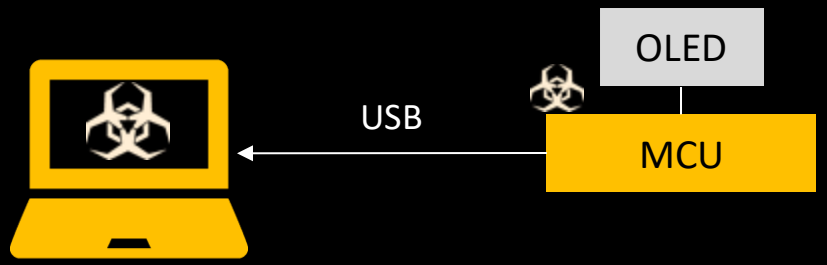
What is a hardware wallet?

https://en.bitcoin.it/wiki/Hardware_wallet

A **hardware wallet** is a special type of bitcoin wallet which stores the user's private keys in a secure hardware device.
They have major advantages over standard software wallets:

- private keys are often stored in a protected area of a microcontroller, and cannot be transferred out of the device in plaintext
- immune to computer viruses that steal from software wallets
- ~~can be used securely and interactively, private keys never need to touch potentially vulnerable software~~
- much of the time, the software is open source, allowing a user to validate the entire operation of the device

TREZOR



https://blog.trezor.io/details-about-the-security-updates-in-trezor-one-firmware-1-6-2-a3b25b668e98

...the buffer overflows, allowing the attacker to write up to 60 bytes of data into a protected part of the memory. Depending on the memory layout the flaw can be escalated to arbitrary code execution...

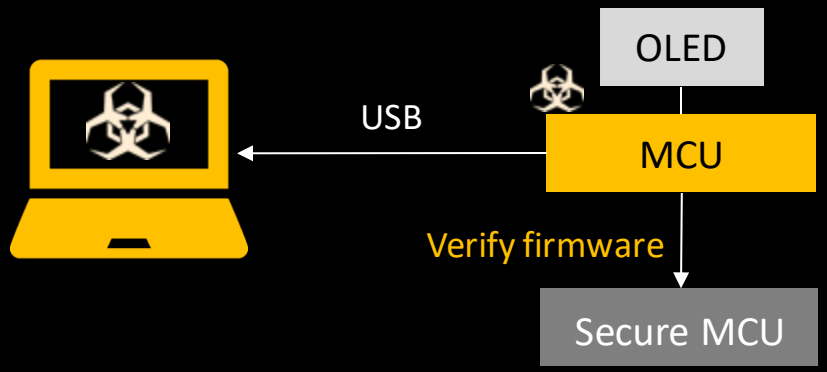
nemanja@hacke.rs

What is a hardware wallet?

https://en.bitcoin.it/wiki/Hardware_wallet

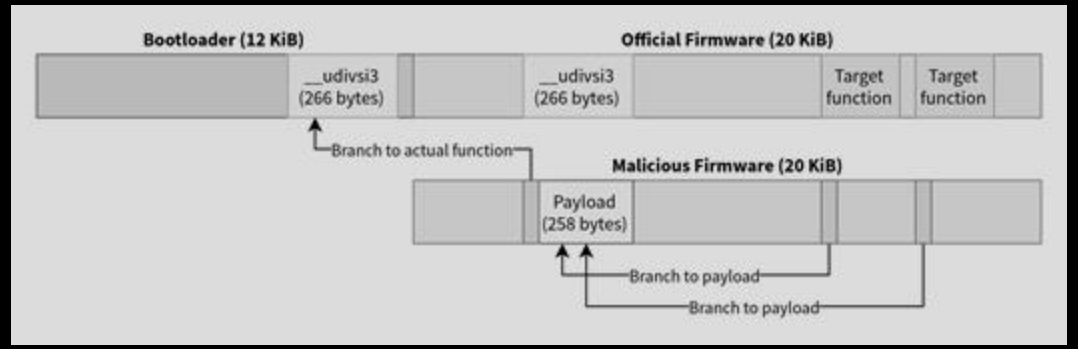
A **hardware wallet** is a special type of bitcoin wallet which stores the user's private keys in a secure hardware device.
They have major advantages over standard software wallets:

- private keys are often stored in a protected area of a microcontroller, and cannot be transferred out of the device in plaintext
- immune to computer viruses that steal from software wallets
- can be used securely and interactively, private keys never need to touch potentially-vulnerable software
- ~~much of the time, the software is open source, allowing a user to validate the entire operation of the device~~



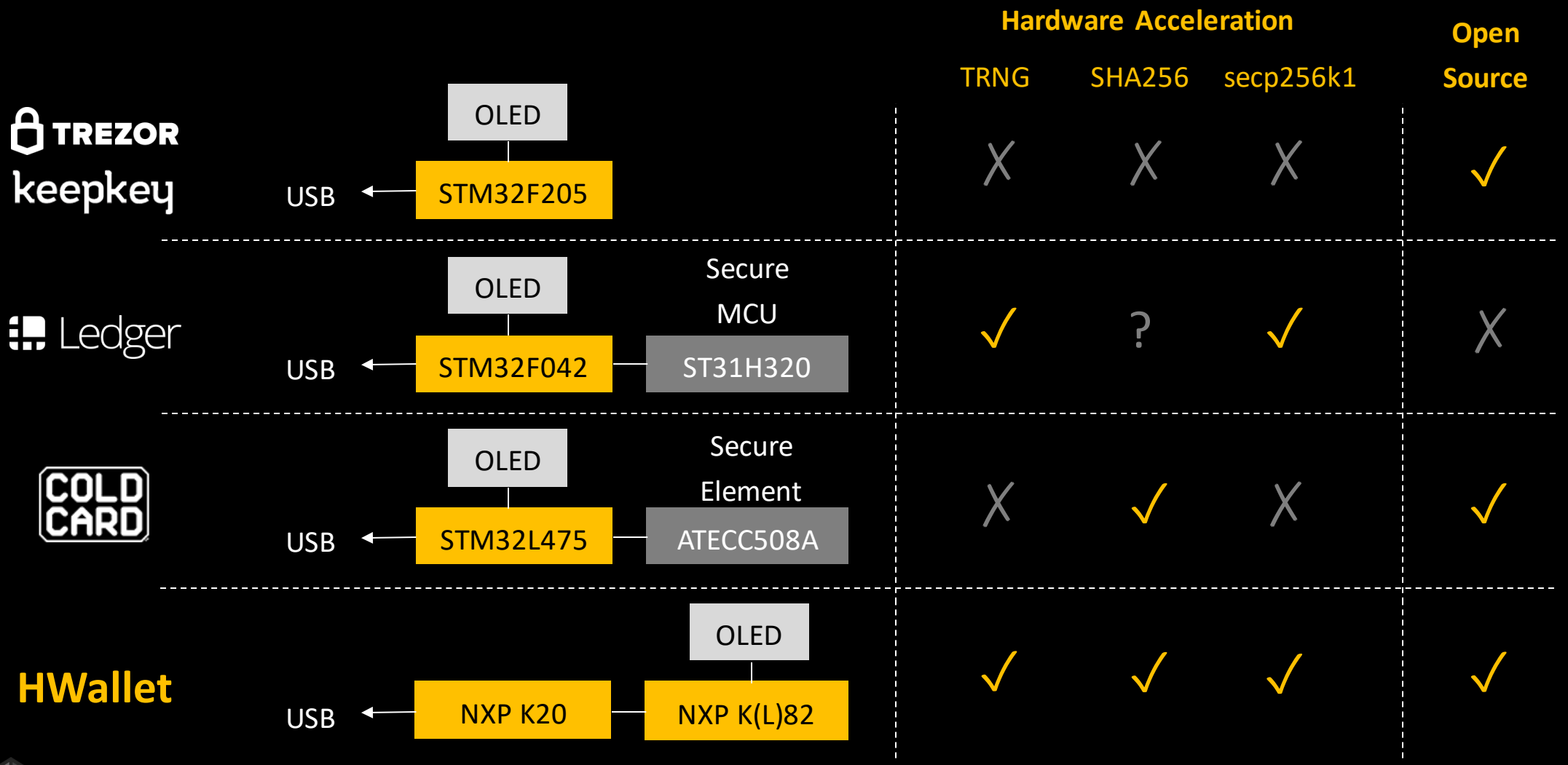
Ledger

https://saleemrashid.com/2018/03/20/breaking-ledger-security-model/



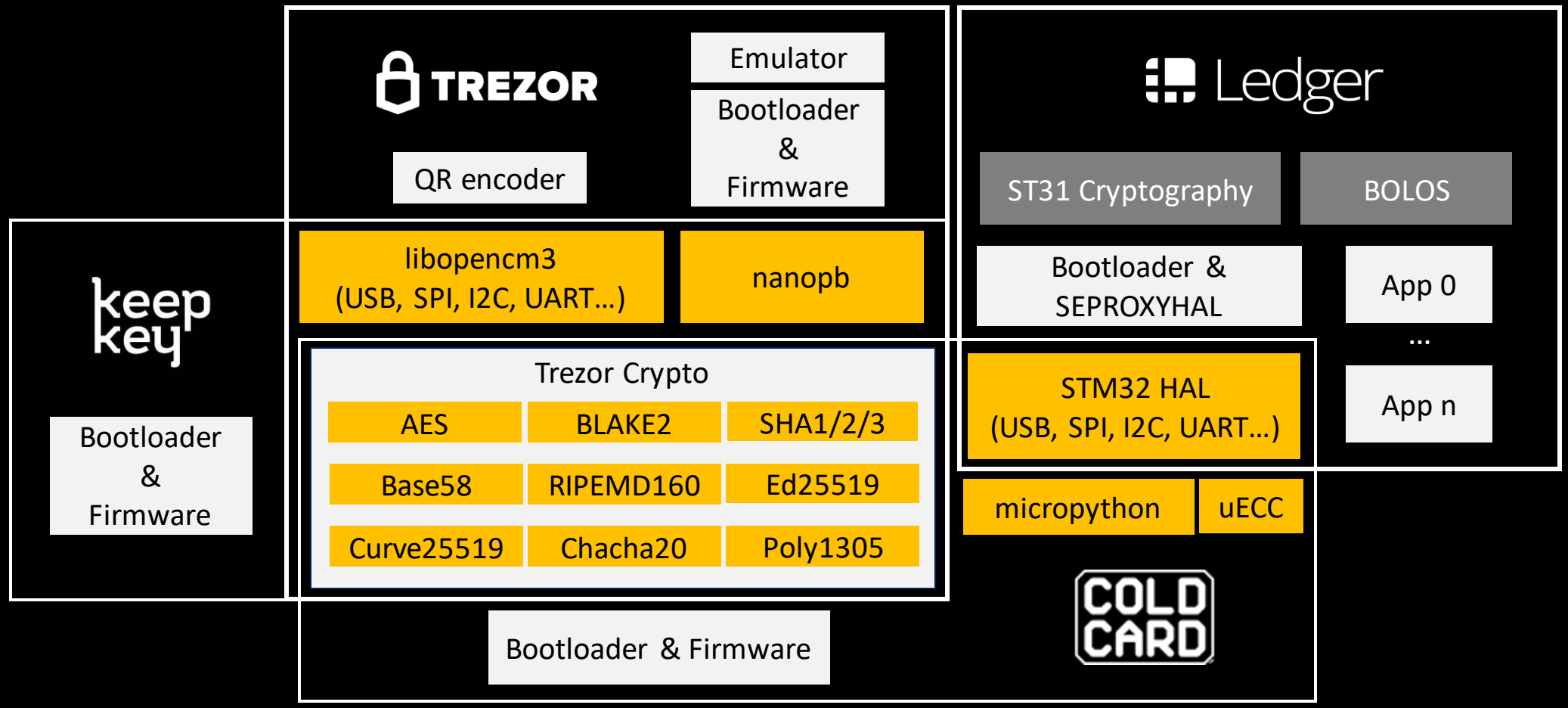
nemanja@hacke.rs

Hardware wallets



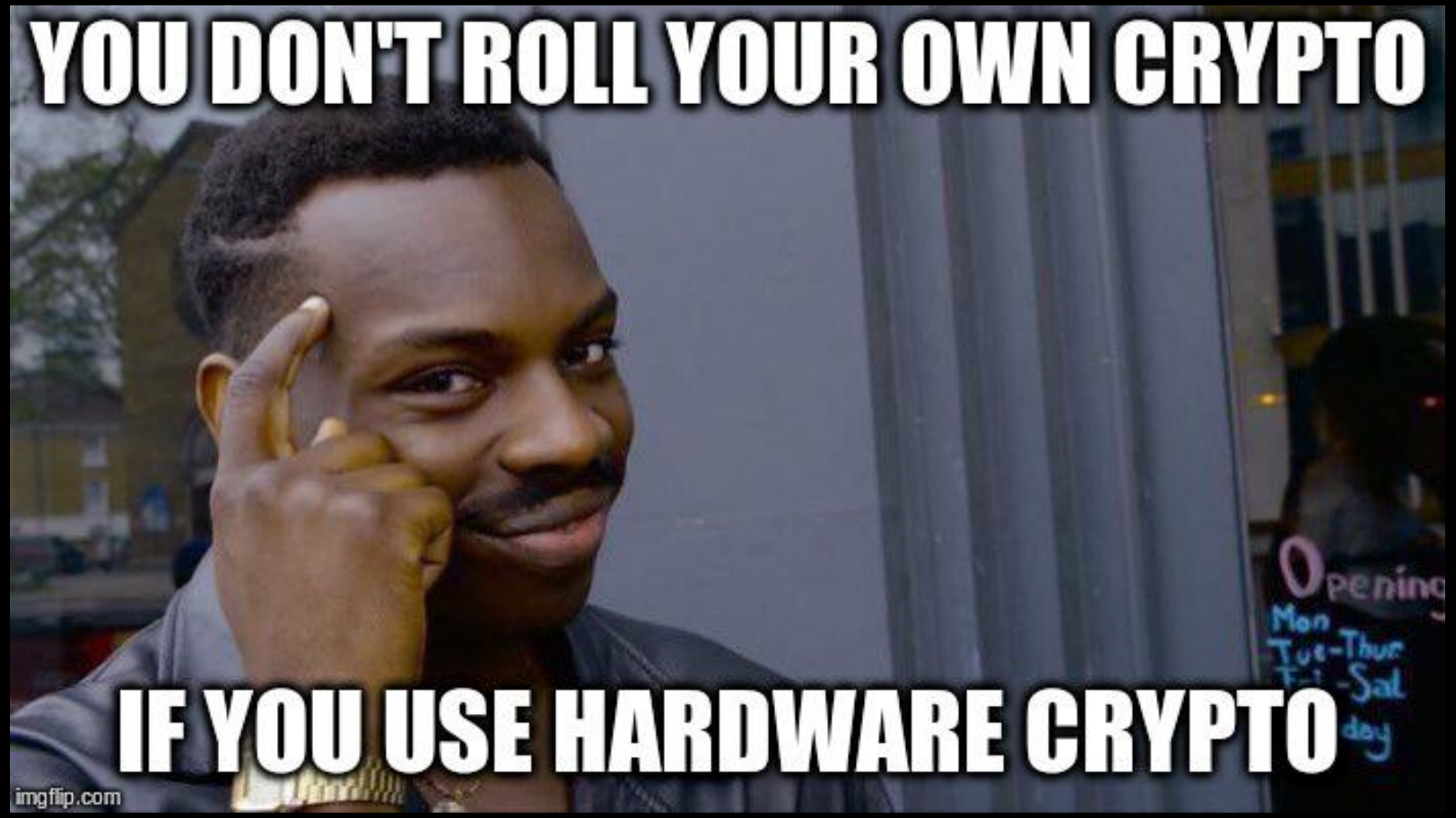
nemanja@hacke.rs

Library dependencies



nemanja@hacke.rs

Don't roll your own crypto!



nemanja@hacke.rs

Code size comparison

COLD CARD

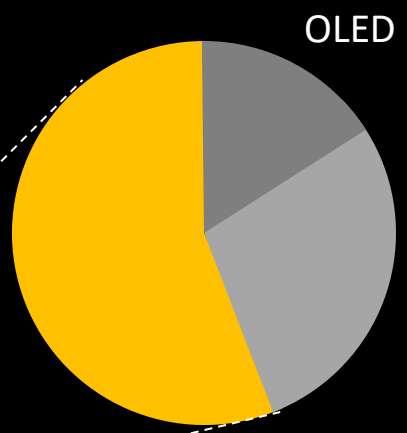
Ledger

TREZOR

keepkey

HWallet

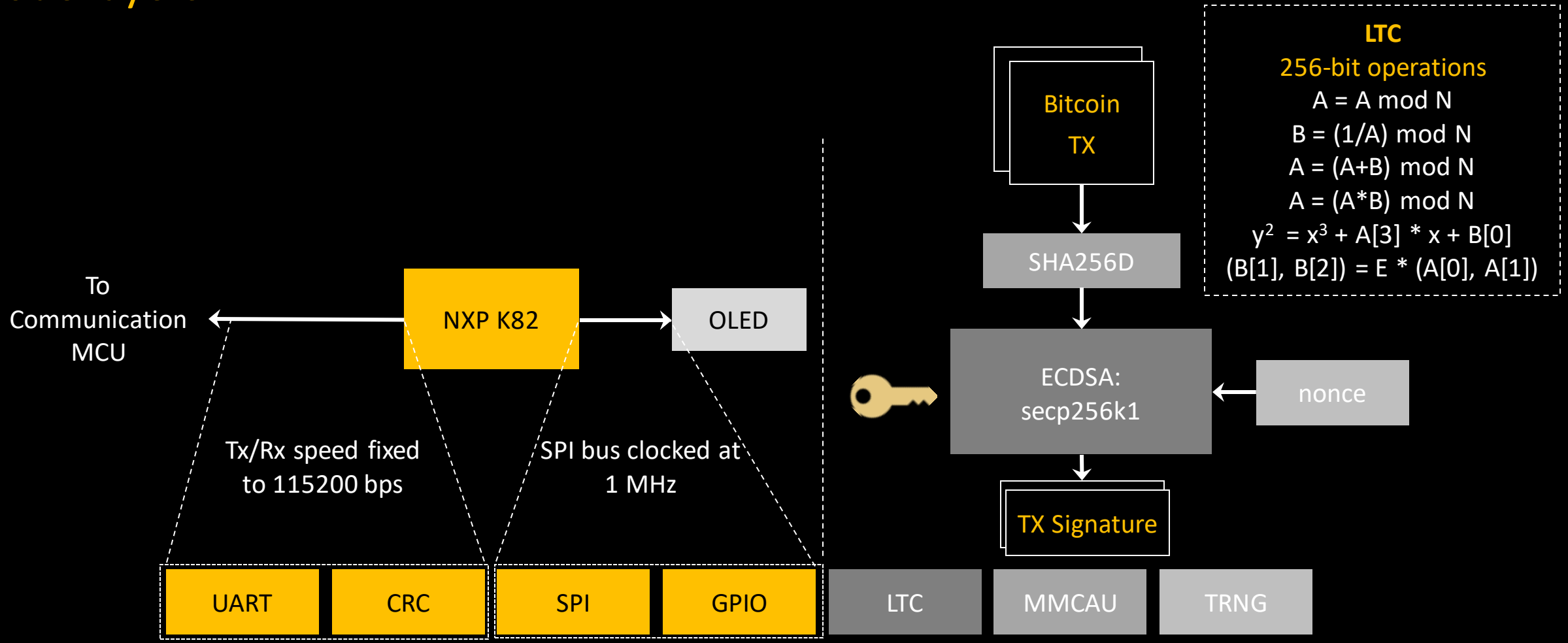
```
git clone https://github.com/{PRODUCT}/{FIRMWARE} --recurse-submodules
cd {FIRMWARE}
wc -l `find ./ -name "*.c" -o -name "*.h"`
```



2.5M+ 346k+ 162k+ 122k+ ~4k

nemanja@hacke.rs

Code layers



https://gitlab.com/nemanjan/hwallet

nemanja@hacke.rs

Code layers

```
typedef struct {
    uint16_t type;
    uint16_t length;
    uint8_t data[32];
    uint32_t crc;
} Packet;

PACKET_Send();
PACKET_Receive();
```

```
typedef struct {
    SPIx* spi;
    GPIOx* dcGpio;
    GPIOx* rstGpio;
    uint8_t dcPin;
    uint8_t rstPin;
    uint8_t buffer[ ];
} OLED;

OLED_WriteRow();
OLED_Clear();
```

```
CRYPTO_Random();
CRYPTO_SHA256();
CRYPTO_ECDSA_Sign();
CRYPTO_ECDSA_GetPublicKey();
typedef struct {
    uint8_t num[32];
    uint8_t len;
} Bignum;
CRYPTO_Bignum_Init();
CRYPTO_Bignum_Mod();
CRYPTO_Bignum_Div();
CRYPTO_Bignum_Sub();
CRYPTO_Bignum_IsNull();
```

B' = (1/B) mod N
A' = A – A mod B
(A/B) mod N = (A'B') mod N

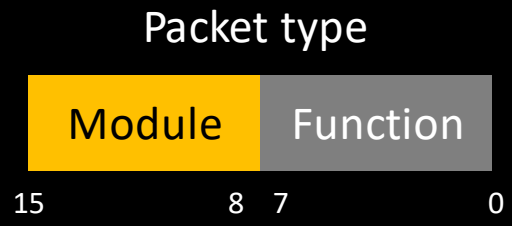
N - a large prime, larger than any A or B, e.g. **p** from secp256k1

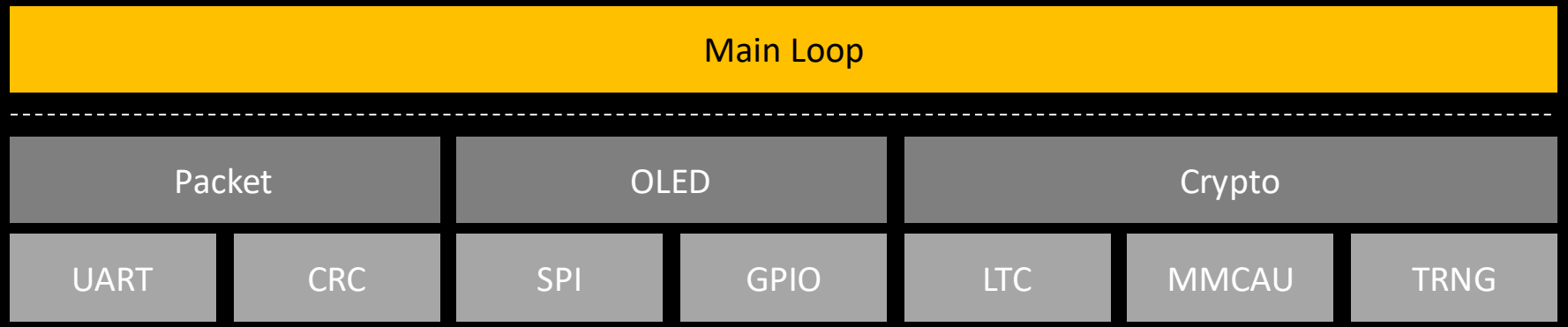
https://gitlab.com/nemanjan/hwallet

nemanja@hacke.rs

Code layers

```
while(1) {
    Packet msg;
    PACKET_Receive(&msg);
    switch(PACKET_MODULE(msg.type)) {
        case PACKET_BITCOIN:
            Bitcoin_Process(&msg);
        ...
    };
}
```



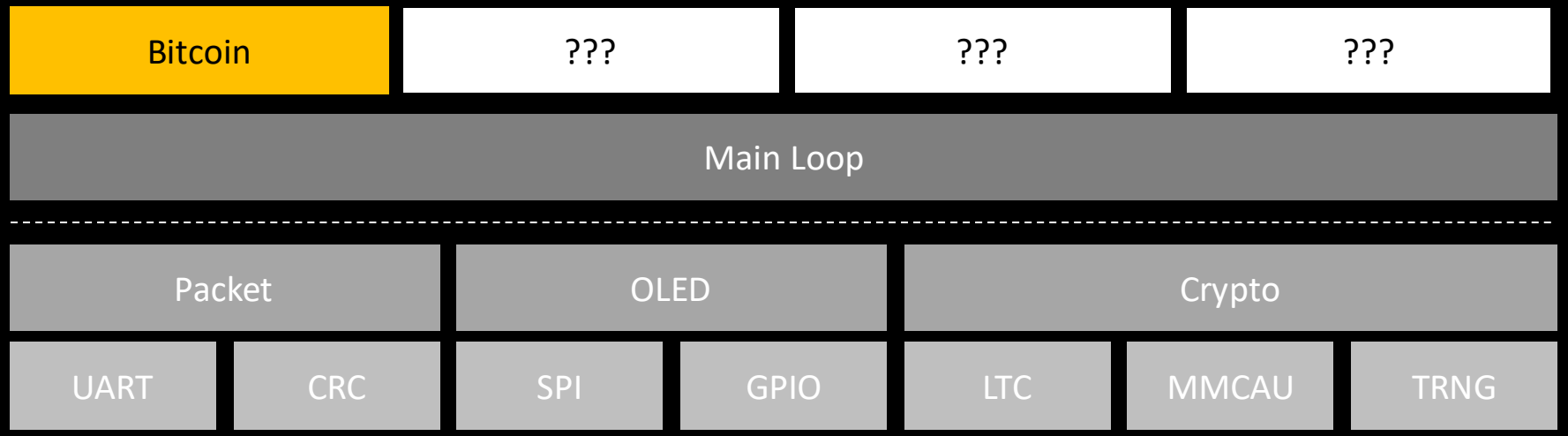


https://gitlab.com/nemanjan/hwallet

nemanja@hacke.rs

Code layers

```
void Bitcoin_Process(Packet* msg) {
    switch(PACKET_FUNC(msg->type)) {
        case BITCOIN_FUNC_INIT_TX:
            Bitcoin_Tx_Init();
        ...
    };
}
```



https://gitlab.com/nemanjan/hwallet

nemanja@hacke.rs

Demo

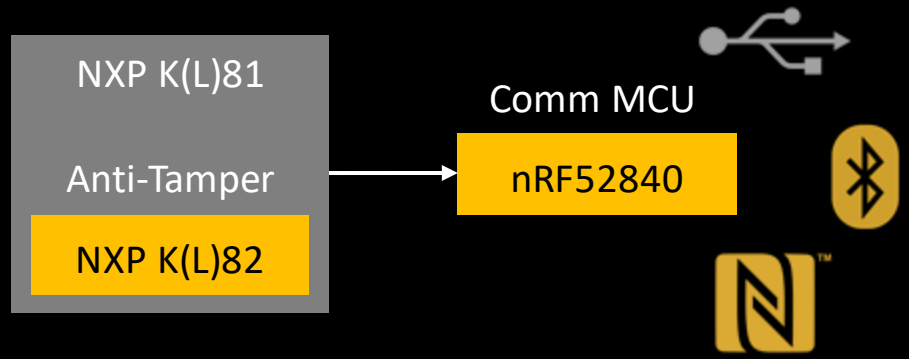
POC||GTFO

nemanja@hacke.rs

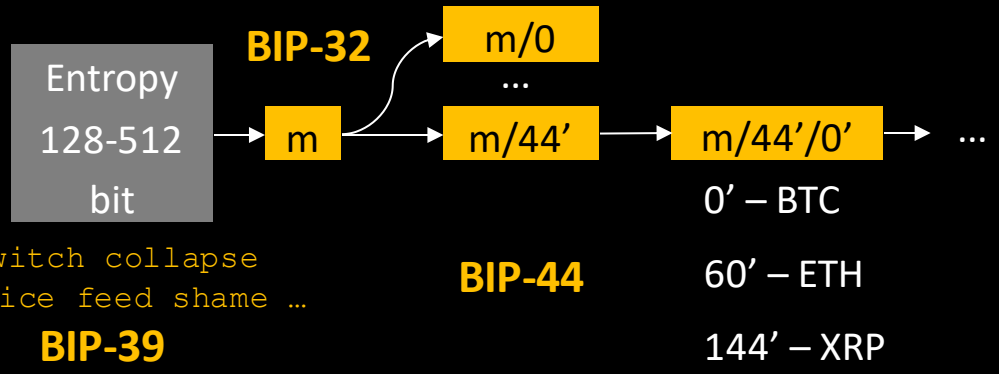
What's next?

FIDO U2F

WebAuthn **CTAP**



Recovery seed



More cryptocurrencies

nemanja@hacke.rs

Questions?