CERIAS

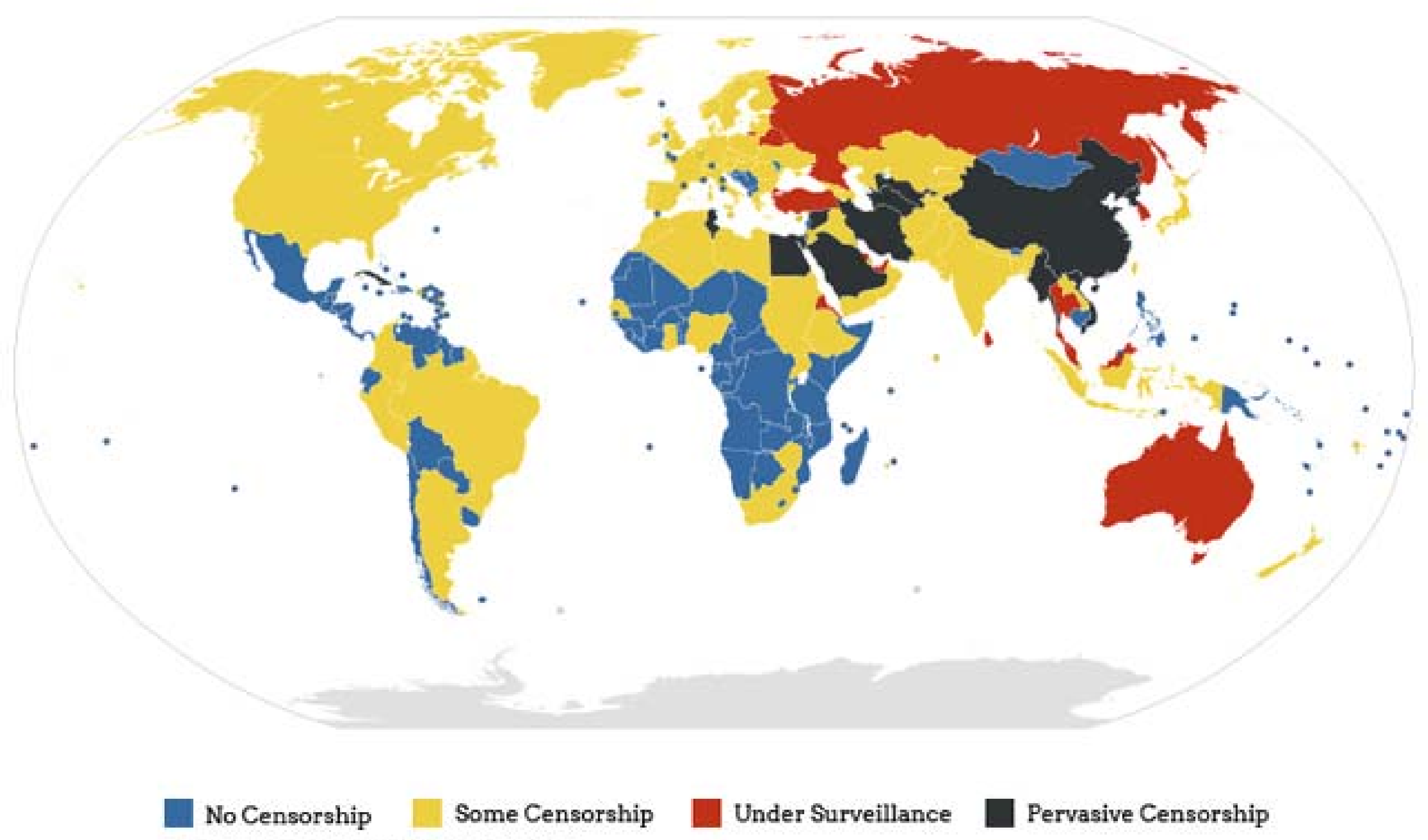
The Center for Education and Research in Information Assurance and Security

Burning Bitcoins for Censorship Resistance

Siddharth Gupta   Aniket Kate   Tim Ruffing

The Article 19 of the Universal Declaration of Human rights –

> *"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers"*

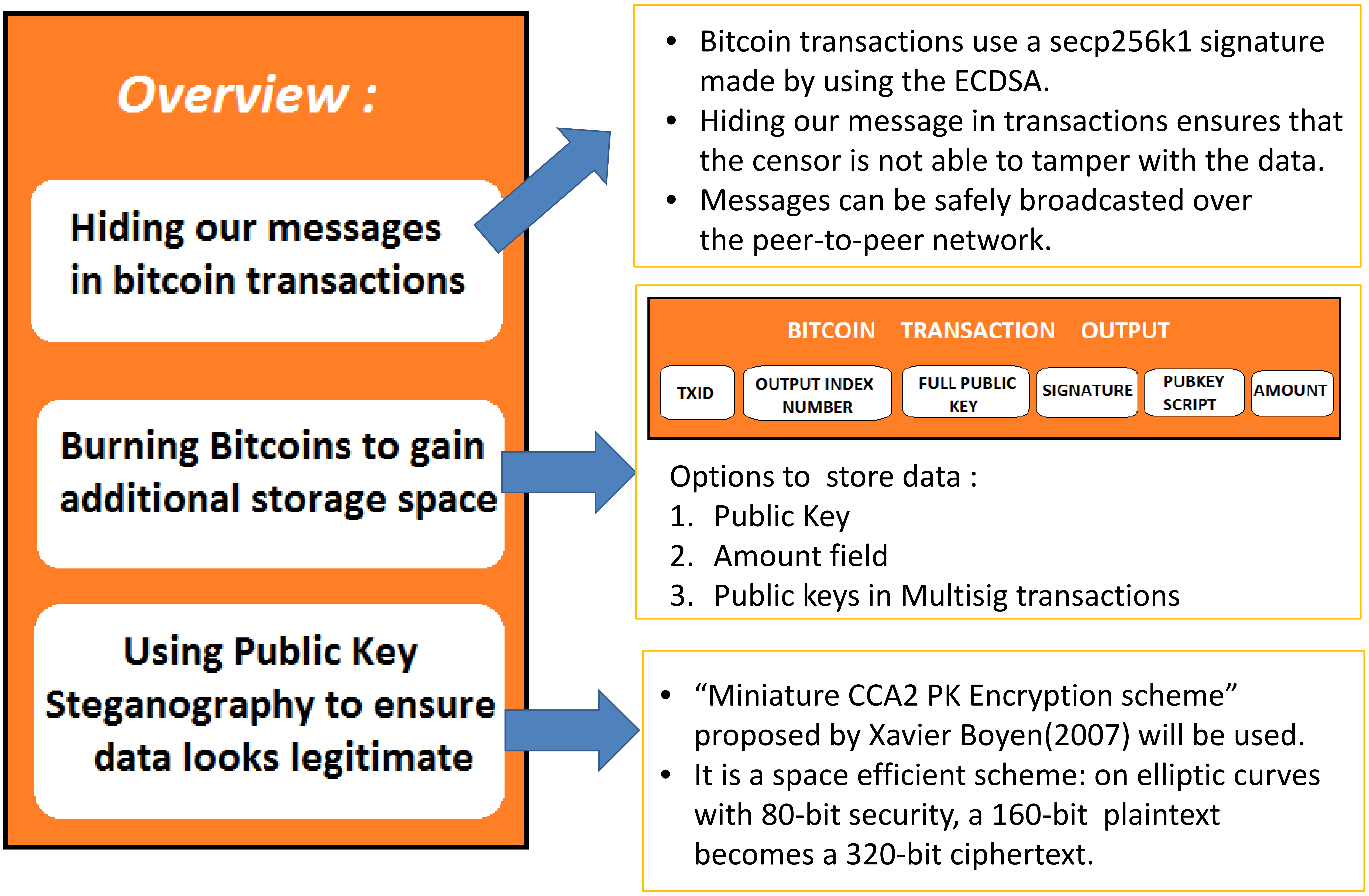


Data Source: Reporters Without Borders

Objective: To create an effective and efficient technique to circumvent internet censorship/ to provide a bootstrap mechanism for existing methods, using the Bitcoin network.

Why use Bitcoins ?

- Economic cost for sensor
- Availability and integrity of data
- Secure communication



Overview :

Hiding our messages in bitcoin transactions

- Bitcoin transactions use a secp256k1 signature made by using the ECDSA.
- Hiding our message in transactions ensures that the censor is not able to tamper with the data.
- Messages can be safely broadcasted over the peer-to-peer network.

Burning Bitcoins to gain additional storage space

BITCOIN TRANSACTION OUTPUT

TXID	OUTPUT INDEX NUMBER	FULL PUBLIC KEY	SIGNATURE	PUBKEY SCRIPT	AMOUNT

Options to store data :

1. Public Key
2. Amount field
3. Public keys in Multisig transactions

Using Public Key Steganography to ensure data looks legitimate

- "Miniature CCA2 PK Encryption scheme" proposed by Xavier Boyen(2007) will be used.
- It is a space efficient scheme: on elliptic curves with 80-bit security, a 160-bit plaintext becomes a 320-bit ciphertext.

CERIAS®

PURDUE UNIVERSITY