RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SEM-M04

CRYPTO BASICS: CIPHERS, TLS AND BLOCKCHAIN

Mike Hamburg

Cryptographer
Rambus Cryptography Research

Crypto 101

Cryptography is the art and science of keeping messages secure

- Crypto building blocks
- Transport security: TLS 1.3
- Attacks on cryptography
- Blockchain and cryptocurrency

This material is heavily borrowed from Ben Jun's crypto 101 talks

CRYPTO BUILDING BLOCKS

the state of being free from threat or danger

Security	Functionality
Confidentiality	Interoperability
Integrity	Performance
Authentication	Usability
Access control	
Non-repudiation	

Confidentiality: encryption

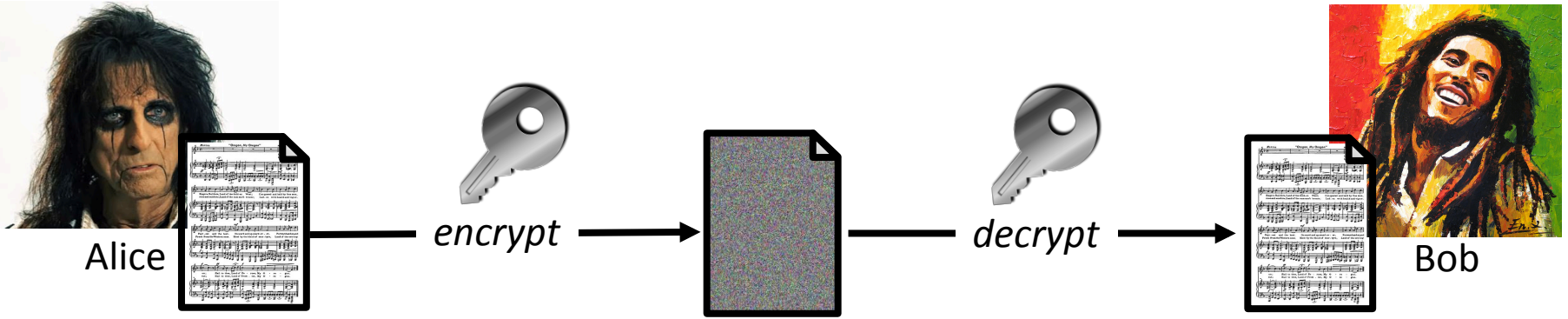
Obfuscation which is easy to undo if you know the secrets, but slow or impossible if you don't

Scytale
ca. 300BC

Alberti disk
1467

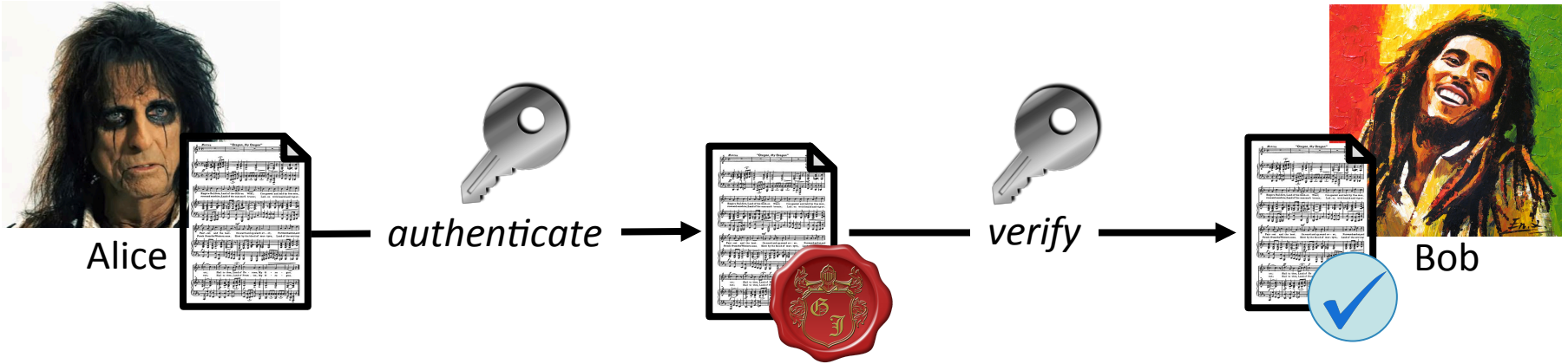
Enigma machine
1923

Symmetric encryption



- Same secret key on both sides
- Convenient and fast
- Cipher isn't secret. Examples: AES, 3DES, ChaCha20

Authenticity

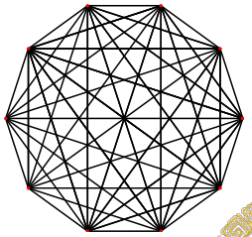


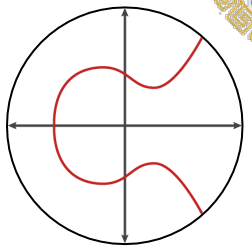
- Examples: HMAC, Poly1305
- Built into some modes: AES-GCM

Scaling cryptography

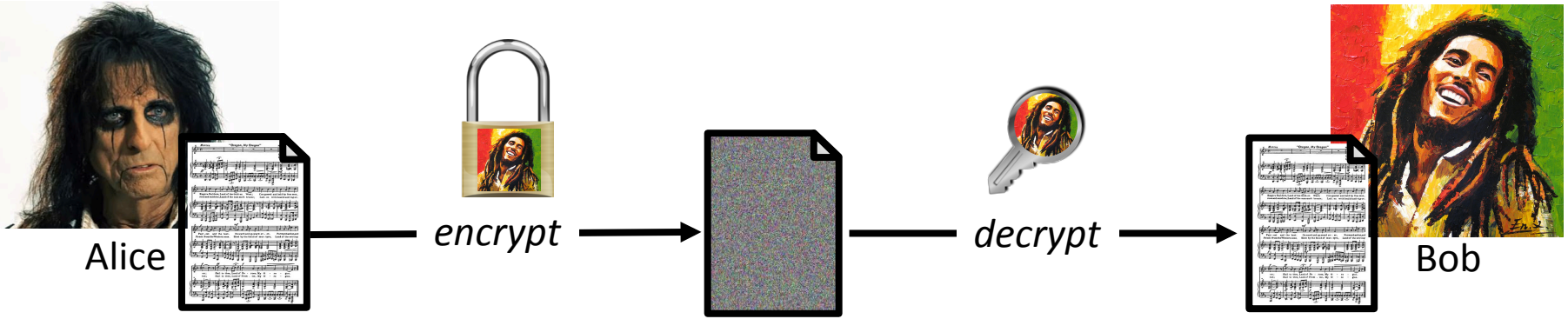
To communicate securely, two parties must share a secret key

- Need $n \choose 2$ keys for n users
  - Billions of devices on the internet: billions^2 keys?
- Or: need a way to securely share a key without meeting
  - Trusted third party: Kerberos
  - Key exchange / asymmetric encryption



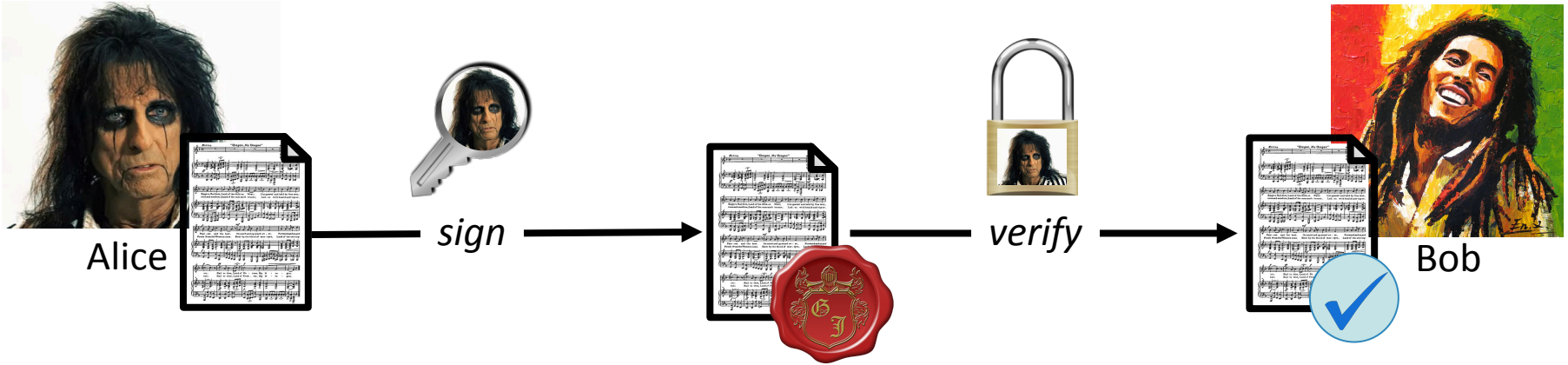


Asymmetric encryption



- One key to encrypt, a different one to decrypt
- Slow and heavy: usually just encrypt a key
- RSA or dedicated key exchange (Diffie-Hellman, ECDH)

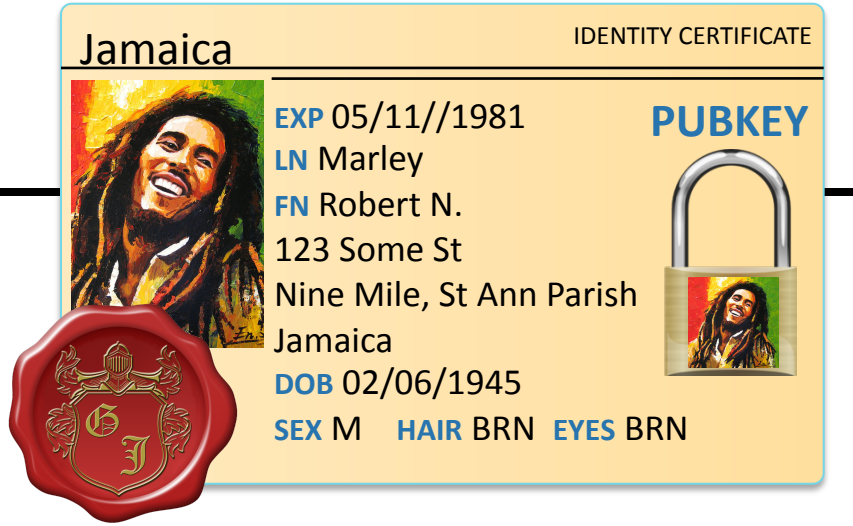
Asymmetric signatures



- Slower and more complex than symmetric auth
- Examples: RSA, ECDSA, EdDSA

Certificates

Alice



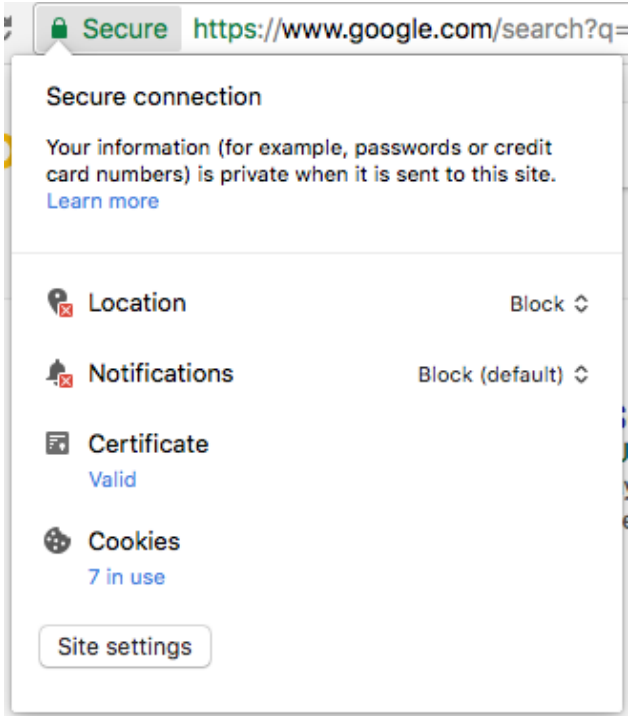
Bob

- Proves Bob's identity and public key to Alice
- Signed by trusted third party (certificate authority)
  - Malicious CA can impersonate Bob, but can't get Bob's keys

SECURE TRANSPORT: TLS 1.3

TLS: backbone of the secure Web

- Descended from SSLv3
  - SSLv1 and v2 were insecure
  - SSLv3 designed by Paul Kocher at CRI
- TLS based on SSLv3 with incremental changes
- TLS 1.3 is biggest change since SSLv3
  - Message flows, ciphers overhauled
  - Significantly simpler



TLS 1.3 handshake (simplified)

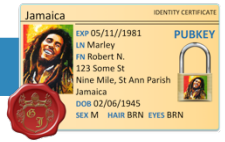
Alice (client)

Options, ephemeral key share

Options, ephemeral key share

Everything past here encrypted and authenticated with shared secret

Certificate, signature on handshake



Application data

Bob.com (server)

Why TLS is secure (simplified)

- From signature on handshake:

  Alice knows someone with $privkey_{Bob}$ performed the handshake

- From certificate on $pubkey_{Bob}$ with Bob's identity:

  Alice knows that $privkey_{Bob}$ belongs to Bob

- From security of key exchange:

  Alice knows that only she and Bob have session key

- From content encryption+auth:

  Alice knows that data is confidential (except for length) and authentic

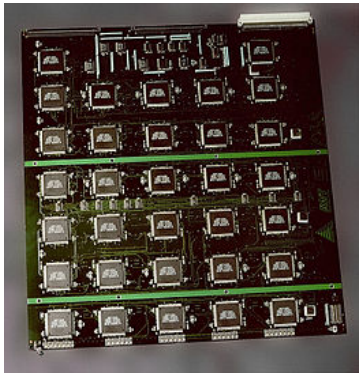
- Alice didn't send cert: Bob only knows that one person sent all the packets

ATTACKS ON CRYPTOGRAPHY

Brute force

- Just try every possible key or password
- Or: simple, well-known mathematical attacks
  - Birthday attack on hashes
  - Rho attack on elliptic curves

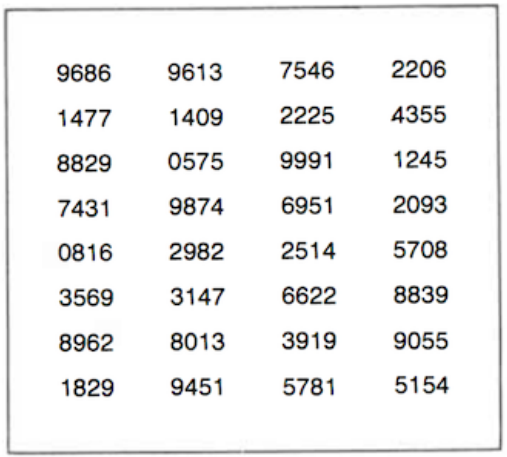
- 2^{80} effort: Bitcoin does this twice a day
- 2^{128} effort: about enough energy to boil the oceans
- 2^{256} effort: requires all the energy in the galaxy



EFF+CRI DES cracker
(2^{56} effort in 1998)

Mathematical break

- History is full of broken ciphers and protocols
  - MD5, SHA-0, SHA-1: collision attacks
  - HDCP 1.0: master key broken
  - Algebraic eraser, extension field discrete log, knapsacks, Cayley-Purser, supersingular curves, LOGJAM, …
- Solution: use heavily-vetted ciphers and protocols
  - AES-GCM, SHA-2, elliptic curves, NaCl, TLS



9686	9613	7546	2206
1477	1409	2225	4355
8829	0575	9991	1245
7431	9874	6951	2093
0816	2982	2514	5708
3569	3147	6622	8839
8962	8013	3919	9055
1829	9451	5781	5154

Original RSA $100 challenge
1977: millions of years?
2017: 8 hours on a workstation

Protocol bugs

- Ciphers must be combined “just so” to create a secure system or protocol

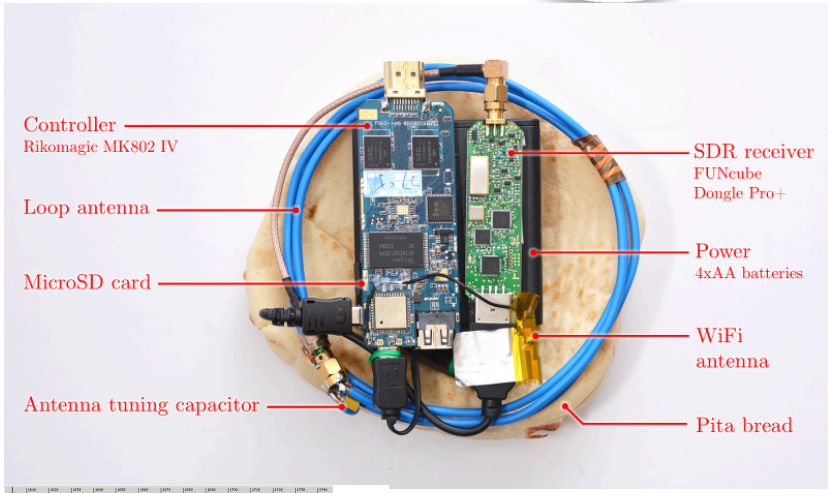
- Protocol downgrade attacks
- Downgrade to export ciphers
- Bliechenbacher RSA padding oracle
- AES-CBC padding oracle

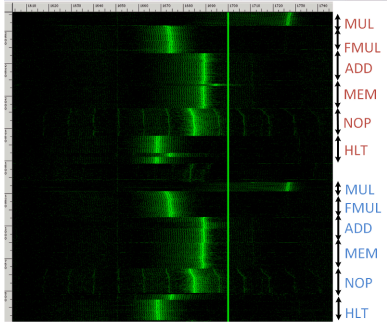
Triple handshake attack
Breaks TLS ≤1.2 without countermeasures

Side channel attacks

- Instead of using cipher output, use extra information
  - Time, power, EM emissions, heat, sound, blinkenlights …
- Cache attack on Linux AES: 65ms

  (Osvik-Shamir-Tromer 2005)
- Rambus security division specializes in side channel defense

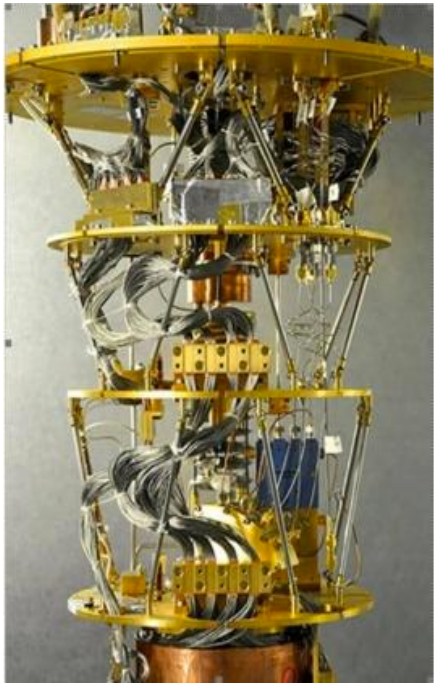




Pita attack
Genkin et al, 2015
Cost: < $500

Quantum computers

- In development. 10-30 years off? Or never?
- Try all the keys at once in quantum superposition!!
  - Not so simple. Only breaks RSA, discrete log, elliptic curves
- Symmetric ciphers still secure with 256-bit key
- NIST post-quantum standards process ongoing



Application bugs

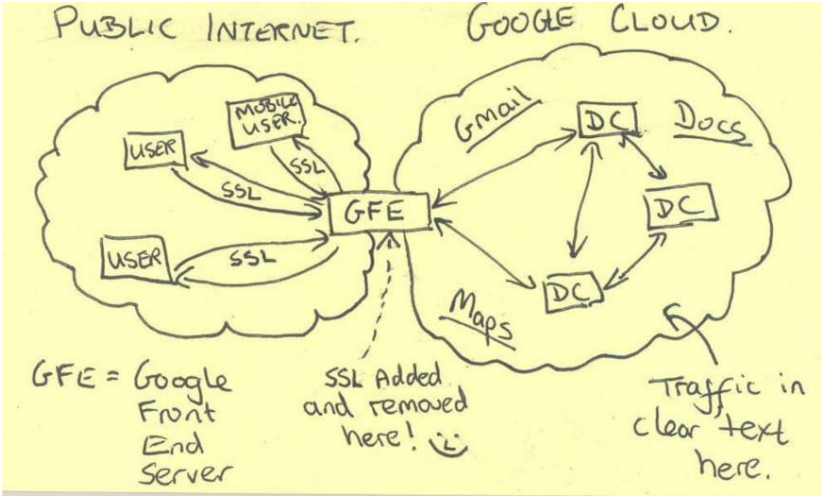
- Nonce reuse
  - Sony PS3 ECDSA signatures
- Buffer overruns
- Not checking certs
  - Apple's "goto fail; goto fail;" bug
- Bad randomness
  - Estonian ID, Taiwanese ID, routers …

Heartbleed (2014)
Buffer overrun
Key disclosure

Work around it

The most common way that crypto is breached

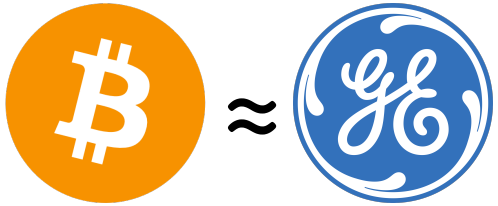
- Compromise the host
- Steal the key
- Steal the plaintext after decryption
- Add backdoor to apps
  - RSA BSAFE, Juniper firewall: DUAL_EC
- Social engineering / insiders
- Get a rogue cert



Snowden leaks, allegedly from NSA (2013)

BLOCKCHAIN AND CRYPTOCURRENCY

Cryptocurrency is a big deal!



Market cap: 120Bn

(+450% from a year ago)

749 coins with market cap > $1MM

Electricity used: 6.6 GW

(also +450% from 1 year ago)

Intro to Bitcoin

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

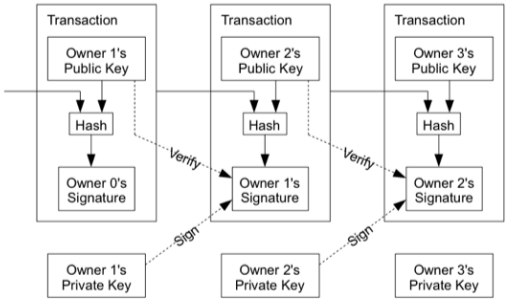
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

"Satoshi Nakamoto" paper (2008)

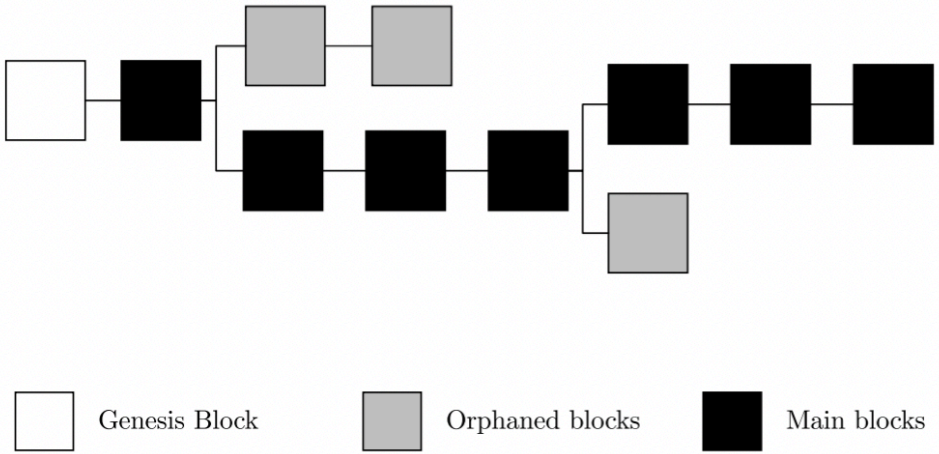
2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.



Blockchain: a permanent distributed ledger

- 10 minutes of mining (brute force SHA256) adds one block
  - Whoever finds it gets a reward
- No centralized control
  - Longest valid chain is canonical
  - If >50% of nodes honest, other nodes (probably) can't rewrite history



Bitcoin: blockchain for transactions

- Wallets identified by hashed ECDSA public key
  - Ledger tracks an account for each wallet
- Sign messages to transfer from one wallet to another
- Once a few blocks have been mined (≈ 30 minutes), transactions probably permanent
  - Prevents double spending

Transactions

0128638b5afb5f3ffb2367dc3dc17261578ae96f05956ab5c38044bf46fa1f0d

(Size: 243 bytes) 2018-04-06 00:51:18

No Inputs (Newly Generated Coins) → 1C1mCxRukix1KfegAY5zQQJV7samAciZpv - (Unspent) 12.79066329 BTC

Unable to decode output address - (Unspent) 0 BTC

12.79066329 BTC

ee5a017d257df5cc91326a26b90a8cb8b0f1948b7697b59927cd853a693aaf90

(Fee: 0.002805 BTC - 188 sat/WU - 752.01 sat/B - Size: 373 bytes) 2018-04-06 00:40:19

16ammK7oA3ZroVe2ekPf8gGwrLdB1UsDLf (0.01628823 BTC - Output)

13nUoLsrMBZKCq3uRUgeJxeMuF2YRcdodd (0.01686707 BTC - Output)

→ 1EX3Taw4a811hqM1wjQgE18ixJERq532zw - (Unspent) 0.01716099 BTC

1MRwYLtXyLXEEsSmQV9Z5KmVyQYpUmybfN - (Unspent) 0.01318931 BTC

0.0303503 BTC

d730c285b0a6880fa092b95ff218c6c6ab1b45d096e94478a7f593fcd94cd8bf

(Fee: 0.00168 BTC - 187.5 sat/WU - 750 sat/B - Size: 224 bytes) 2018-04-06 00:40:31

1JsyLU5LDPzQHUmh64QD7iNjAWxdu34dJB (3.54416305 BTC - Output)

→ 3BMEX5afR5a1H449sHRsYrZ1vaRfyB7j1v - (Unspent) 0.2984238 BTC

14y7B1xBikdFqrzL3Vb5UoyEMu2pG6HfB6 -

Currency?

- Future: instantly, anonymously send money anywhere in the world!

- Present: little connection between cryptocurrency and real value
  - Need more cryptocurrency-denominated futures contracts, rents, markets
  - Too slow and unscalable to replace banking / credit card networks
  - Mainly for speculation; also research and crime
  - 749 coins with market cap > $1MM. Which one(s) will stick around?

- Environmental cost: better alternative to mining?

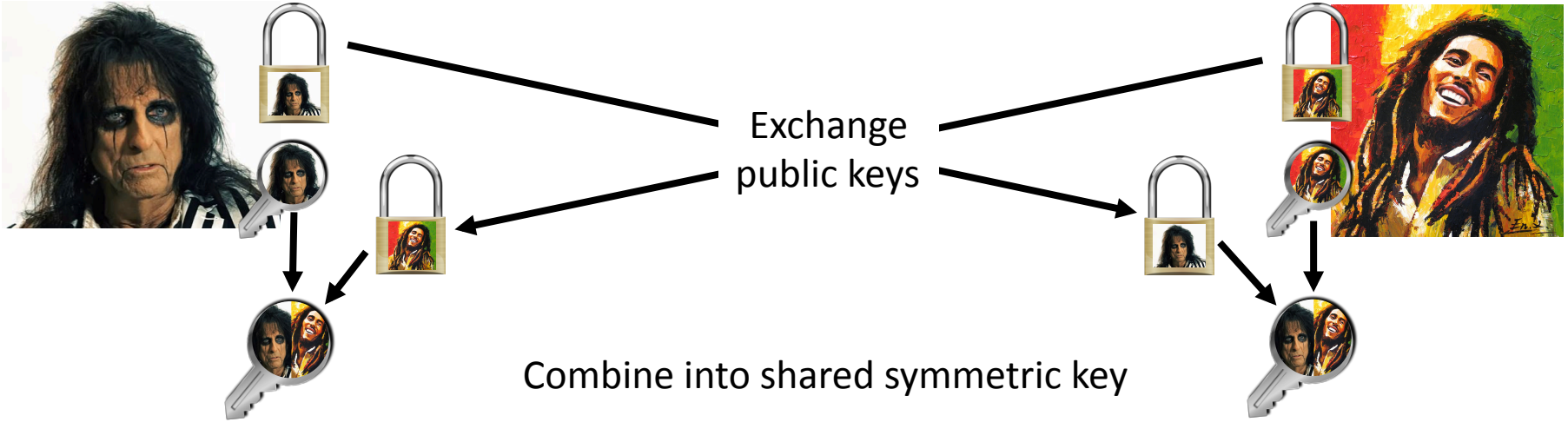
Just scratching the surface

- Anonymity vs pseudonymity
- Smart contracts: transfer coins only if conditions are met
- Consensus protocol
  - Proof-of-work
  - Proof-of-stake
  - Byzantine agreement
- ASIC vs GPU mining
- Quantum resistance

WRAP UP

QUESTIONS?

Key exchange



- Examples: Diffie-Hellman, ECDH / X25519

Functionality, safety and security

Functionality: product must work correctly under normal circumstances

Safety: product must work correctly or fail gracefully even in extreme circumstances

Security: product must work correctly or fail gracefully even when being actively attacked

Security vs functionality in crypto

Security

- Confidentiality
- Integrity
- Authentication
- Access control
- Non-repudiation

Functionality

- Interoperability
- Performance
- Usability

- Note for future use: Bitcoin consumes more electricity (58TWh/year) than Massachusetts (53) and almost as much as Maryland (60). Possibly will be Maryland by when I give the top
- Up 5.5x (from 10.4) year on year
- https://digiconomist.net/bitcoin-energy-consumption
- Market cap of all cryptocurrencies was ~800B at peak, between Alphabet and Apple
- 2^{80} work every 12 hours