Cryptographic Protocols

Algorithms vs. Protocols

Algorithm

A mathematical procedure used to transform data.

Protocol

A series of steps and message exchanges between multiple entities to achieve a specific cryptographic result.

Example Protocols

WPA2
Restricts wifi access to authorized users, and encrypts their traffic.

SSL/TLS
Verifies the identity of a web server, and encrypts traffic to and from that server.

Bitcoin
Allows the secure and decentralized transfer of value from one account to another.

Creating a Protocol

- Identify your objective(s)
- Understand your data
- Methodically look for openings
- Find ways to plug the openings

Creating a Protocol

- Identify your objective(s)
- Create data flow diagram
- STRIDE x elements
- Attack trees
  - Aim for 100% mitigation

WPA2:
WiFi Protected Access, v2

Block unauthorized users
Protect authorized users

WPA2 Objectives

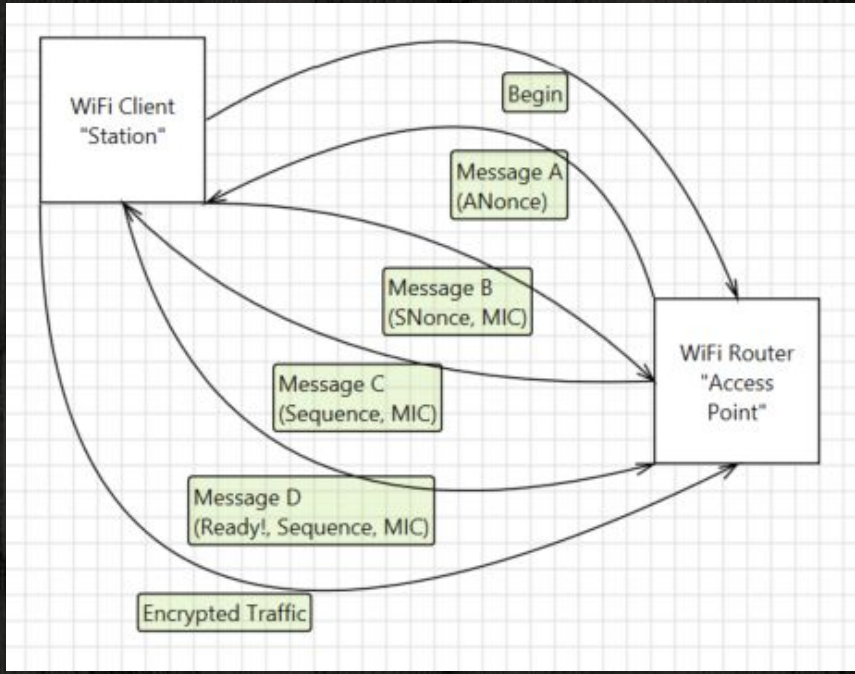
- Verify identity of client
- Verify identity of router
- Encrypt against external listeners
- *Non-goal:* Encrypt against internal listeners
- Do all this on cheap hardware

Possible Solutions

- Encrypt packets with shared key
  - Strong key isn’t human-friendly
- Client generates key
  - How to transmit securely to router?

Only solution is for client and router to collaboratively generate unique key.

“Four-way Handshake”



Key = PRNG (
PWD + ANonce + SNonce + AMAC + SMAC
)

STRIDE x Elements

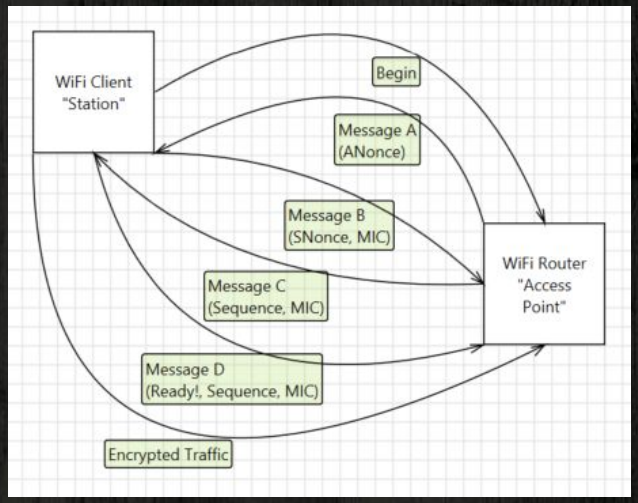
	S	T	R	I	D	E
Processes	√	√		√	√	√
External Interactors	√					
Data Stores	√	√		√	√	
Data Flows		√	√	√	√	

Just external interactors and data stores.

Repudiation = not applicable
Denial of service = out of scope

STRIDE x Elements

- Spoof Client
- Spoof Router
- Tamper Messages A-D
- ID Messages A-D
- Tamper Encrypted Traffic
- ID Encrypted Traffic



WPS = Satan

“Let’s replace the passphrase with an 8-digit PIN…
...well, 7 digits, because one is a checksum…
...and since 8 digits are hard to remember, we’ll tell you which half you got right!”

SSL/TLS:
Secure Sockets Layer/ Transport Layer Security

Verify server identity
Protect HTTP traffic

SSL Objectives

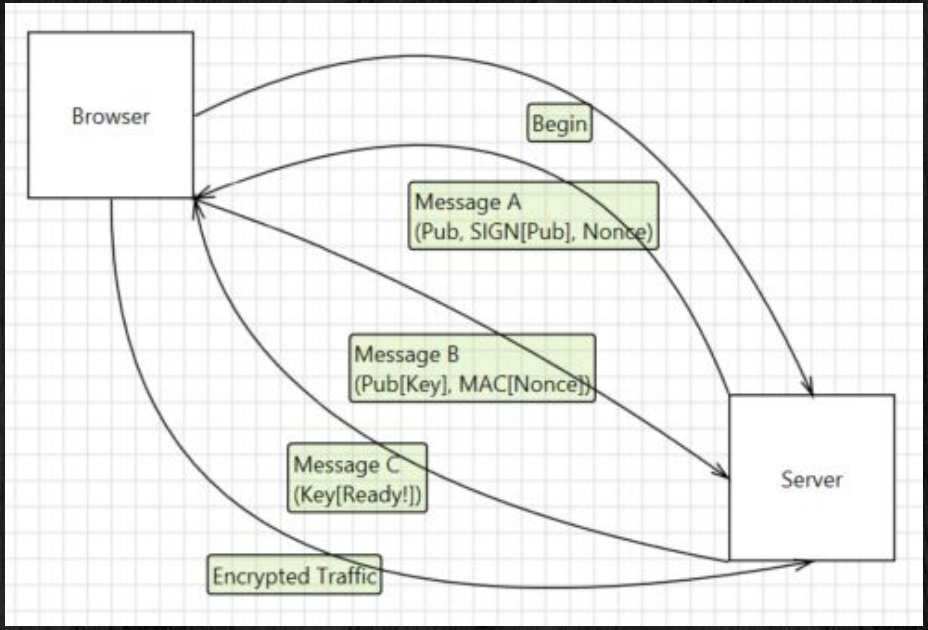
- Verify identity of server
- *Non-goal:* Verify identity of client
- Encrypt against MITM listeners
  - Including MITM on client
- Full resources of client and server available

Possible Solutions

- Generate a key similar to WPA2
  - Every other user would know it
- Server could generate key
  - No shared secret with client

Client generates key, then submits it to server encrypted with public half of server's asymmetric encryption key.

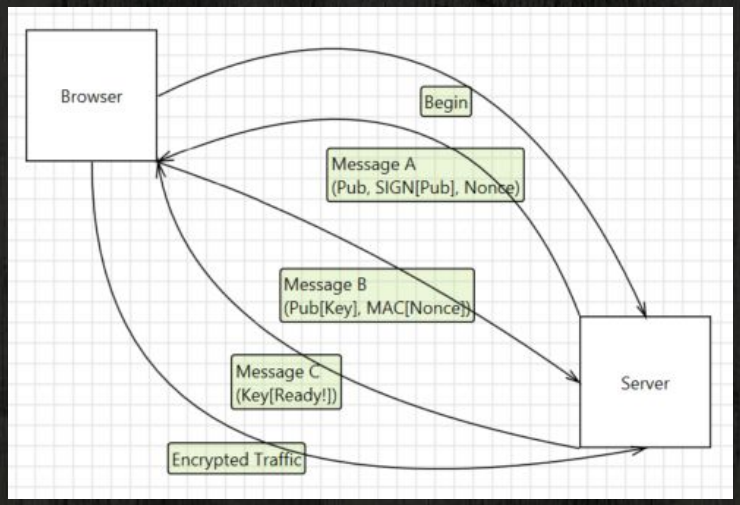
SSL/TLS Key Exchange



SIGN[X] = Priv[H[X]]

STRIDE x Elements

- Spoof Server
- Tamper Messages A-C
- ID Messages A-C
- Tamper Encrypted Traffic
- ID Encrypted Traffic



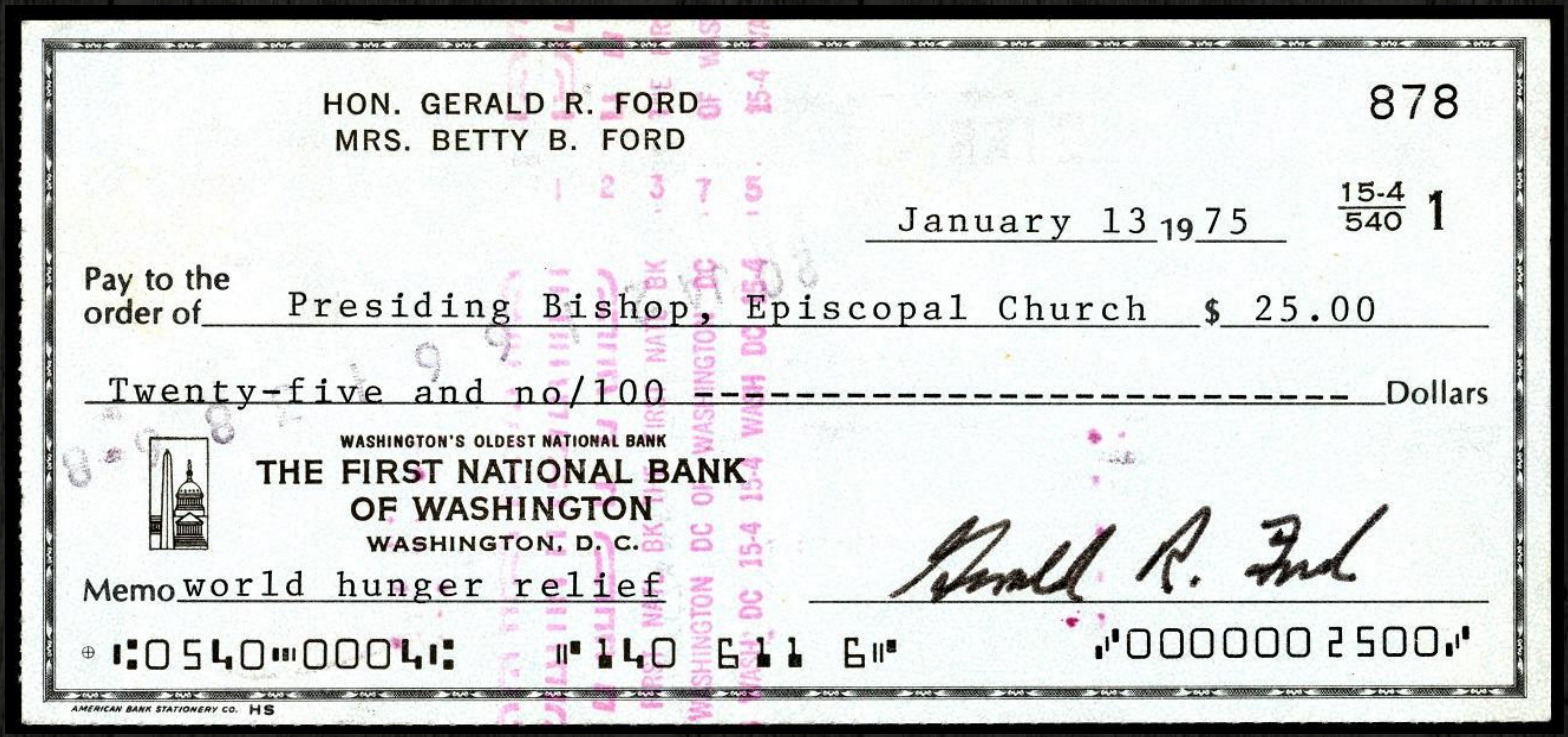
Bitcoin

Securely transfer value from one account to another...
...without a central authority

Bitcoin Objectives

- Alice can transfer value to Bob
- Eve cannot transfer value from Alice without Alice's permission
- Alice cannot repudiate the transfer
- The transfer isn't secret… but it's secret-*ish*
- No central authority
  - Can't fail or be compromised
  - Cannot create new currency ("gold standard")

Possible Solutions



HON. GERALD R. FORD
MRS. BETTY B. FORD

878

January 13 1975

15-4
540 1

Pay to the order of Presiding Bishop, Episcopal Church $ 25.00

Twenty-five and no/100 ---------- Dollars

WASHINGTON'S OLDEST NATIONAL BANK
THE FIRST NATIONAL BANK
OF WASHINGTON
WASHINGTON, D. C.

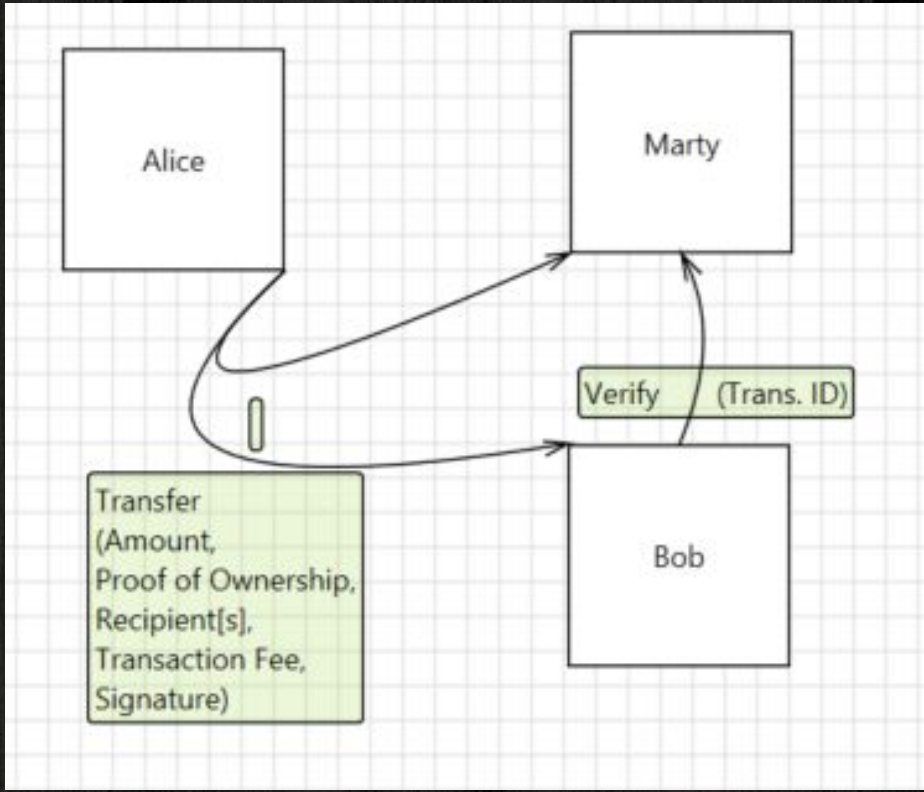
Memo world hunger relief

Gerald R. Ford

⑆054000041⑆ ⑈140 611 6⑈ ⑈0000002500⑈

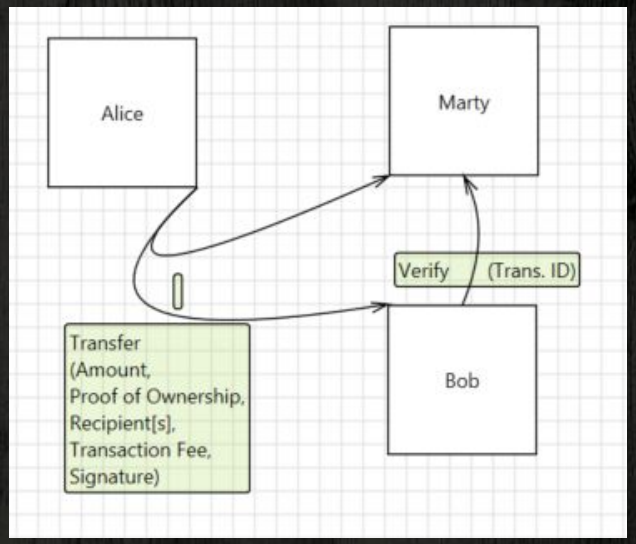
AMERICAN BANK STATIONERY CO. HS

Bitcoin, Step 1: Transactions

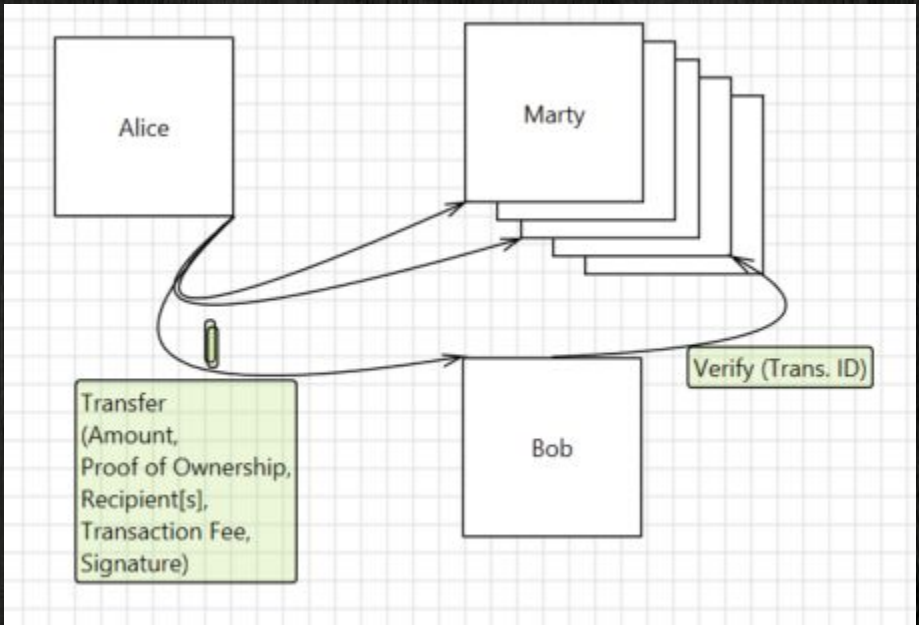


STRIDE x Elements

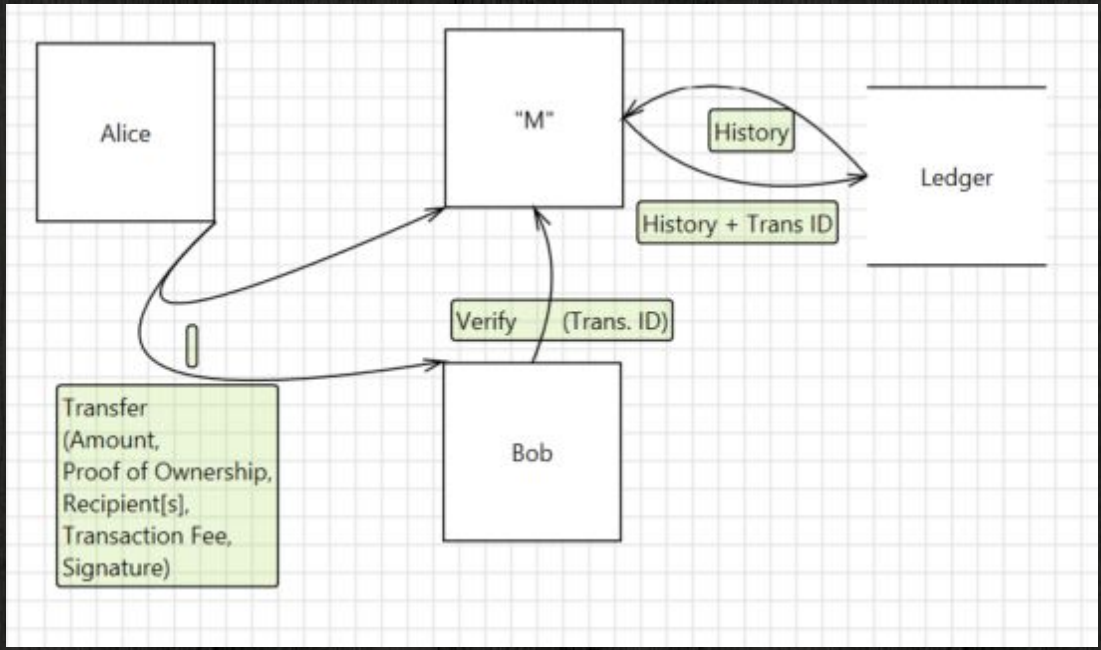
- Spoof Alice
- Spoof Bob
- Tamper with transfer
- Spoof Marty …
- Repudiate transfer …



Bitcoin, Step 2: Verification

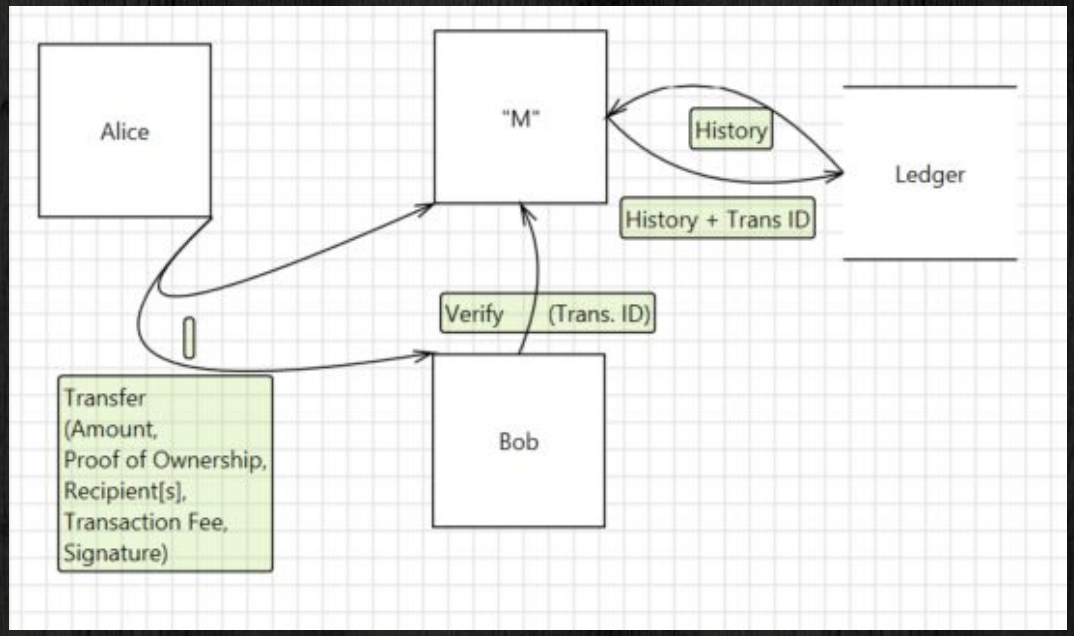


Bitcoin, Step 3: Update Ledger

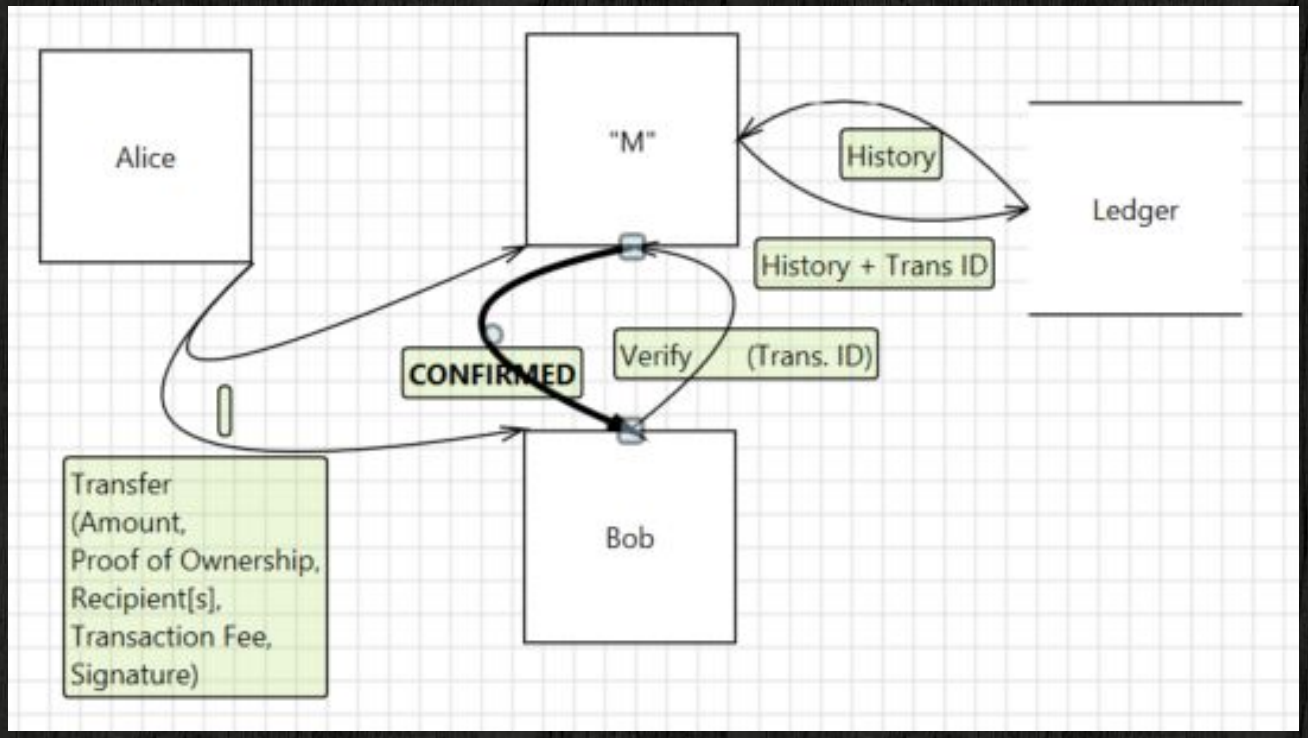


STRIDE x Elements

- Spoof “M”
- Repudiate transfer



Bitcoin, Step 4: Confirmation



Confirmation takes 6 blocks (~1 hour),
to minimize risk of forks.

Creating a Protocol

A protocol is effectively just a program written in a human language. To create one…

- Identify your objective(s)
- Understand your data
- Methodically look for openings
- Find ways to plug the openings

But reuse existing ones where possible!