Town Crier

Authenticated Data Feeds For Smart Contracts

CS5437 Lecture by Kyle Croman and Fan Zhang
Mar 18, 2016

Smart Contract

- Decentralized App: Programs are executed by all miners who reach consensus about the resulting state (i.e. the side effects)
- Ethereum supports Turing-complete languages
- Smart contracts have persistent storage on the blockchain
- But, a smart contract has no access to the world outside of the blockchain
    - “What’s the closing price of APPL on March 11, 2016.”
- An Example of Town Crier:
    - “The closing price of APPL on March 11, 2016 is $102.26. Here is a cryptographic proof asserting that the aforementioned data is correctly obtained from https://finance.yahoo.com/ and delivered to you by Town Crier.”
    - A smart contract can efficiently verify the integrity of data.

Trusted Hardware

- Intuition: a secure box.
- Once loaded with a program, it will be executed in the secure box with good guarantees [against software adversaries, including OS]:
  - Secrecy: Nobody gets to observe the internal state
  - Integrity: Nobody can interfere with the execution of the program
- How about **loading**?
  - Loading itself is not secure (has to be done by OS on current platforms)
  - **Solution: check the result of loading [remote attestation]**
- Intel Software Guardance eXtension (SGX)
  - The secure box in SGX is called an **enclave**.
  - Implemented by 24 new instructions
  - Available on Skylake CPUs
  - Not perfect. See Intel SGX Explained for more details.

Remote Attestation

With an remote attestation, an SGX host can prove to anyone that

- It has genuine Intel SGX
- The initial state (state after loading) of the enclave is ***M***

The idea of remote attestation is simple,

- Intel buries a secret key to every SGX-enabled CPU
- An attestation is just a **digital signature** of M under the SGX secret key

$$att = M || \sigma_{\mathsf{sk}_{\mathsf{sgx}}}(M)$$

Root of Trust

- Trust **Intel** for:
- Correctly implemented of SGX semantics.
- Correctly implemented Remote Attestation mechanism.
- Correctly distributed secret keys.
- ...

Restrictions of SGX

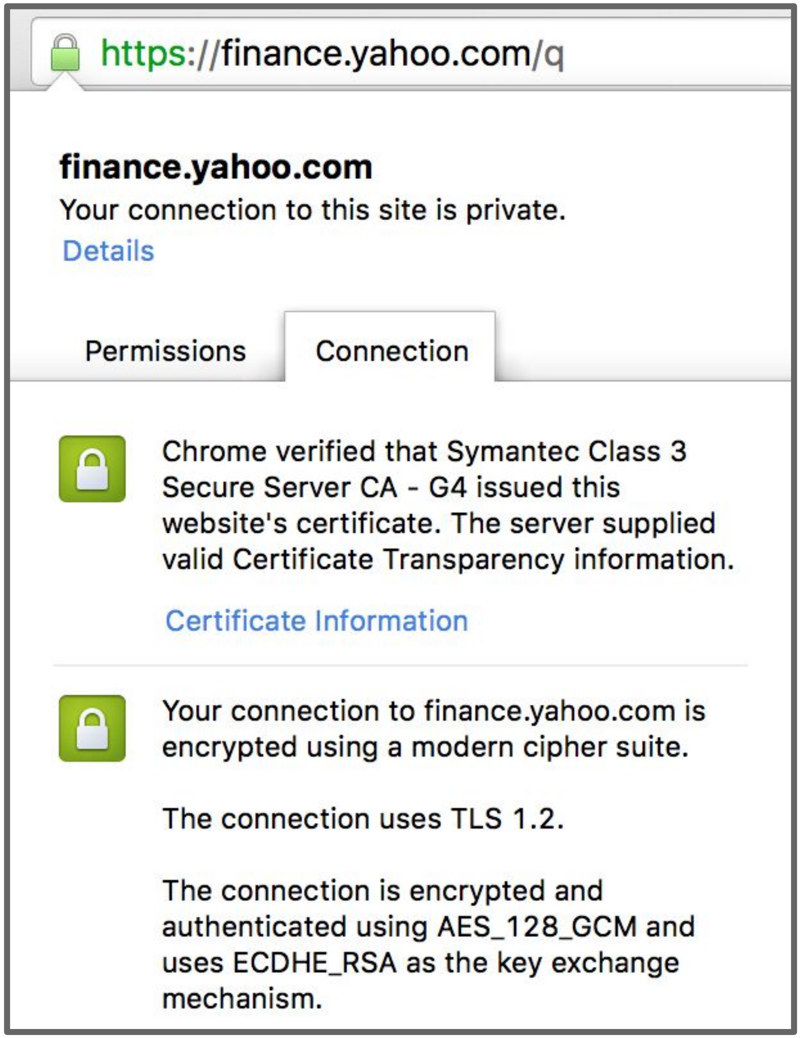
- Many restrictions are imposed for security reason / easier implementation
- Basically, C/C++ program, but
- Only non-privileged (ring3) instructions is allowed in an enclave, which means
  - No OS service anymore (wall clock time, PRNG (e.g. /dev/random)
  - No I/O (printf, open, socket, etc.)
- Workarounds
  - For networking,
  - SGX provides trusted time and RAND

Town Crier: the goal

- “The closing price of APPL on March 11, 2016 is $102.26. Here is a cryptographic proof asserting that the aforementioned data is correctly obtained from https://finance.yahoo.com/ and delivered to you by Town Crier.”
- Provide authenticated data feed to smart contracts.
- **Authenticity**, with which one can verify
  - The source of the message
  - That the message is not altered during transmission.
- We have awesome tools to achieve authenticity over Internet:
  - Transport Layer Security (TLS)

HTTPS / TLS

- TLS provides authenticity by means of MAC.
- One can easily verify the authenticity of an TLS connection by checking the website's *certificate* and the MAC.



https://finance.yahoo.com/q

finance.yahoo.com

Your connection to this site is private.

Details

Chrome verified that Symantec Class 3 Secure Server CA - G4 issued this website's certificate. The server supplied valid Certificate Transparency information.

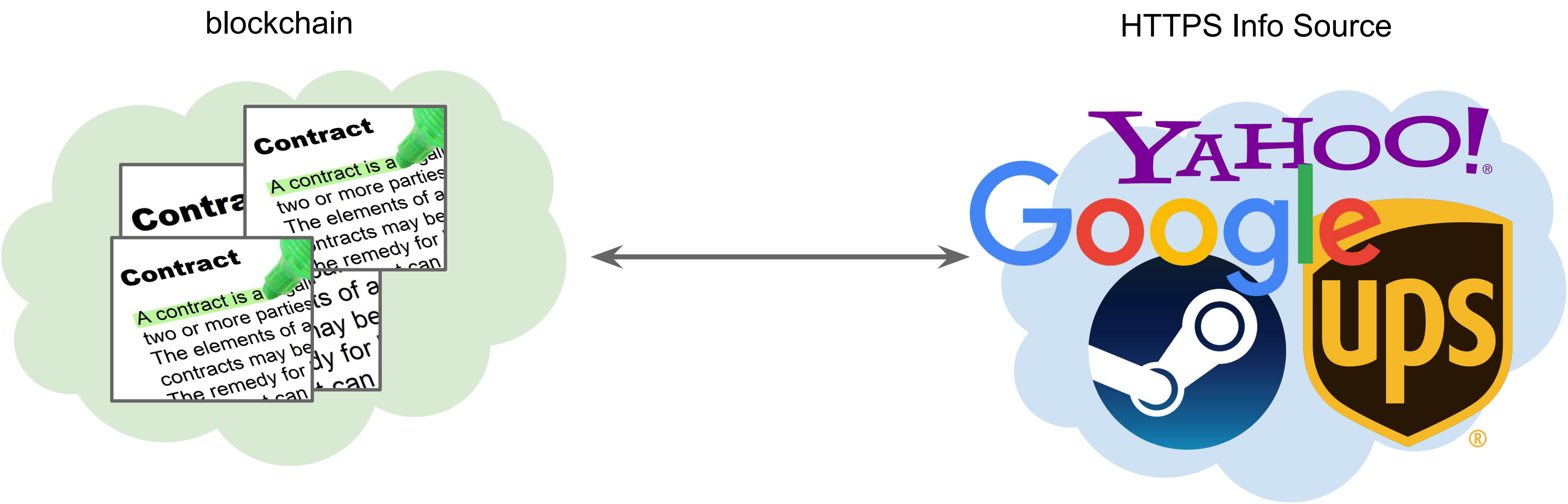
Certificate Information

Your connection to finance.yahoo.com is encrypted using a modern cipher suite.

The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.

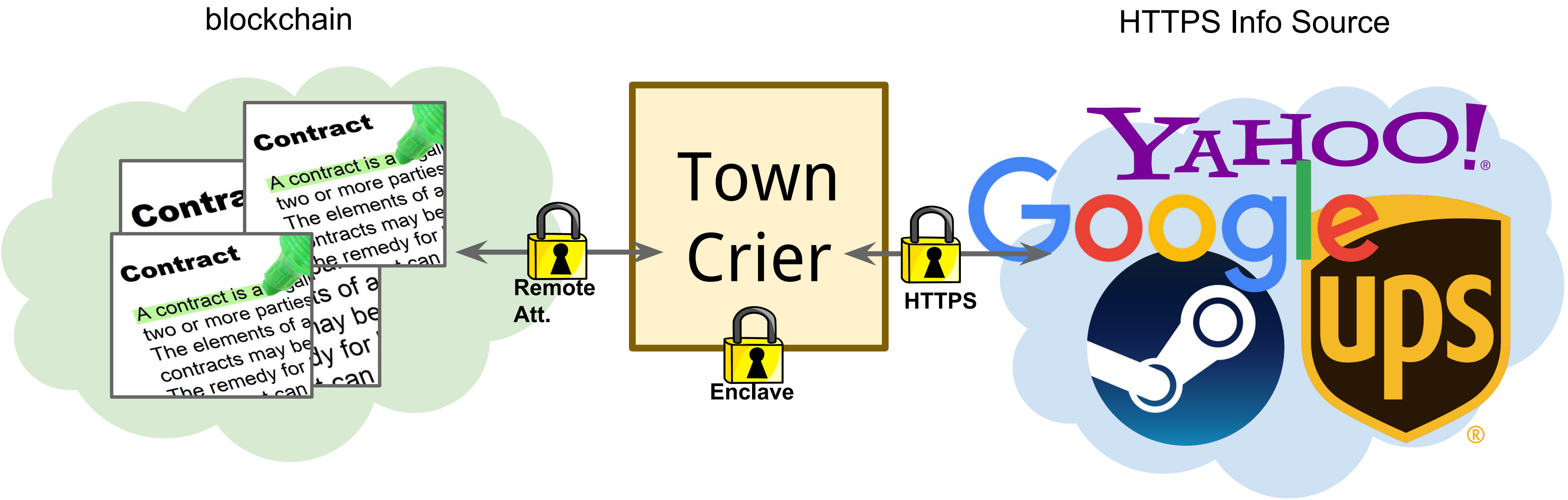
Town Crier: the idea



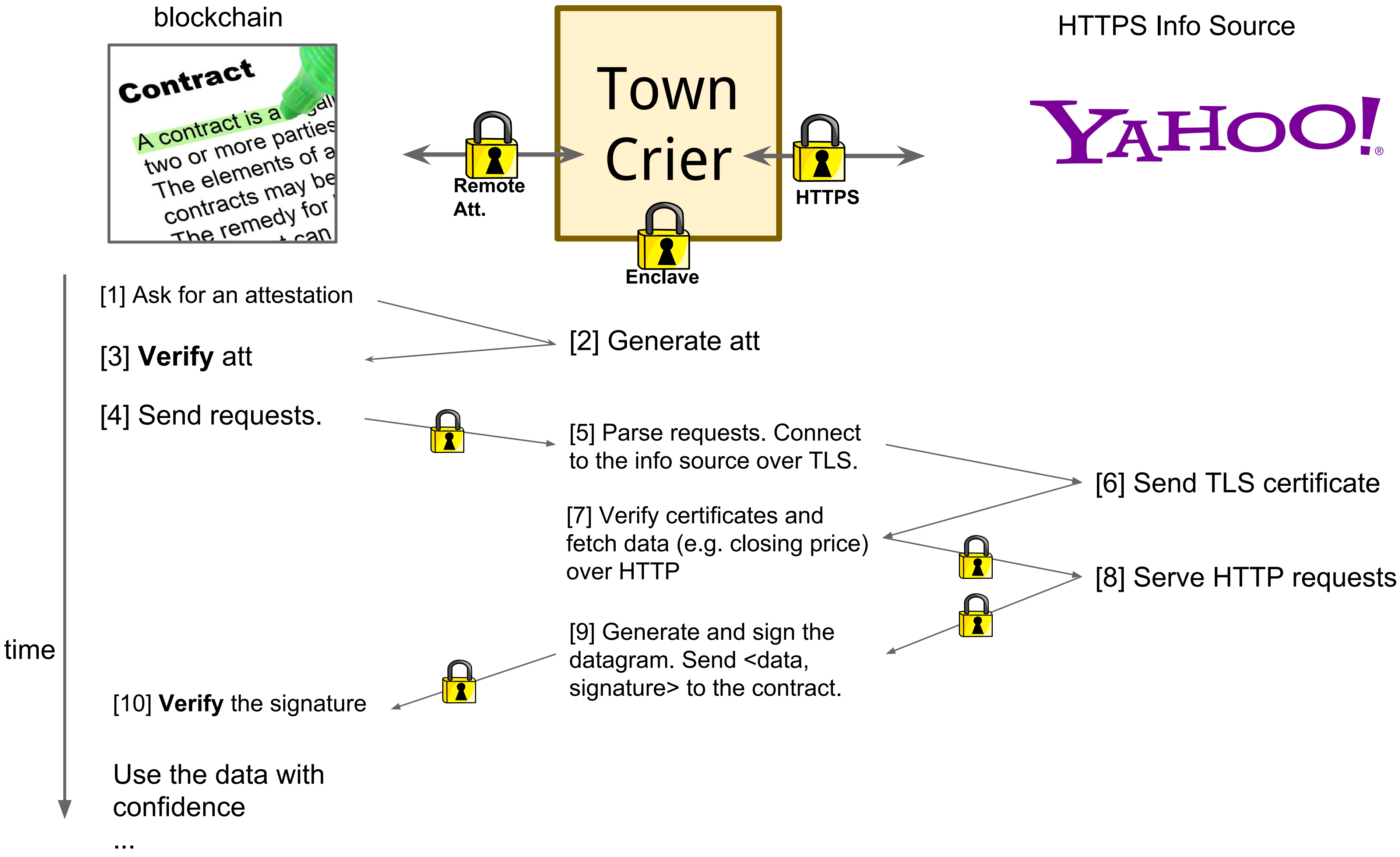
blockchain

HTTPS Info Source

Town Crier: the idea



Chain of Authenticity: an example



[1] Ask for an attestation

[2] Generate att

[3] **Verify** att

[4] Send requests.

[5] Parse requests. Connect to the info source over TLS.

[6] Send TLS certificate

[7] Verify certificates and fetch data (e.g. closing price) over HTTP

[8] Serve HTTP requests

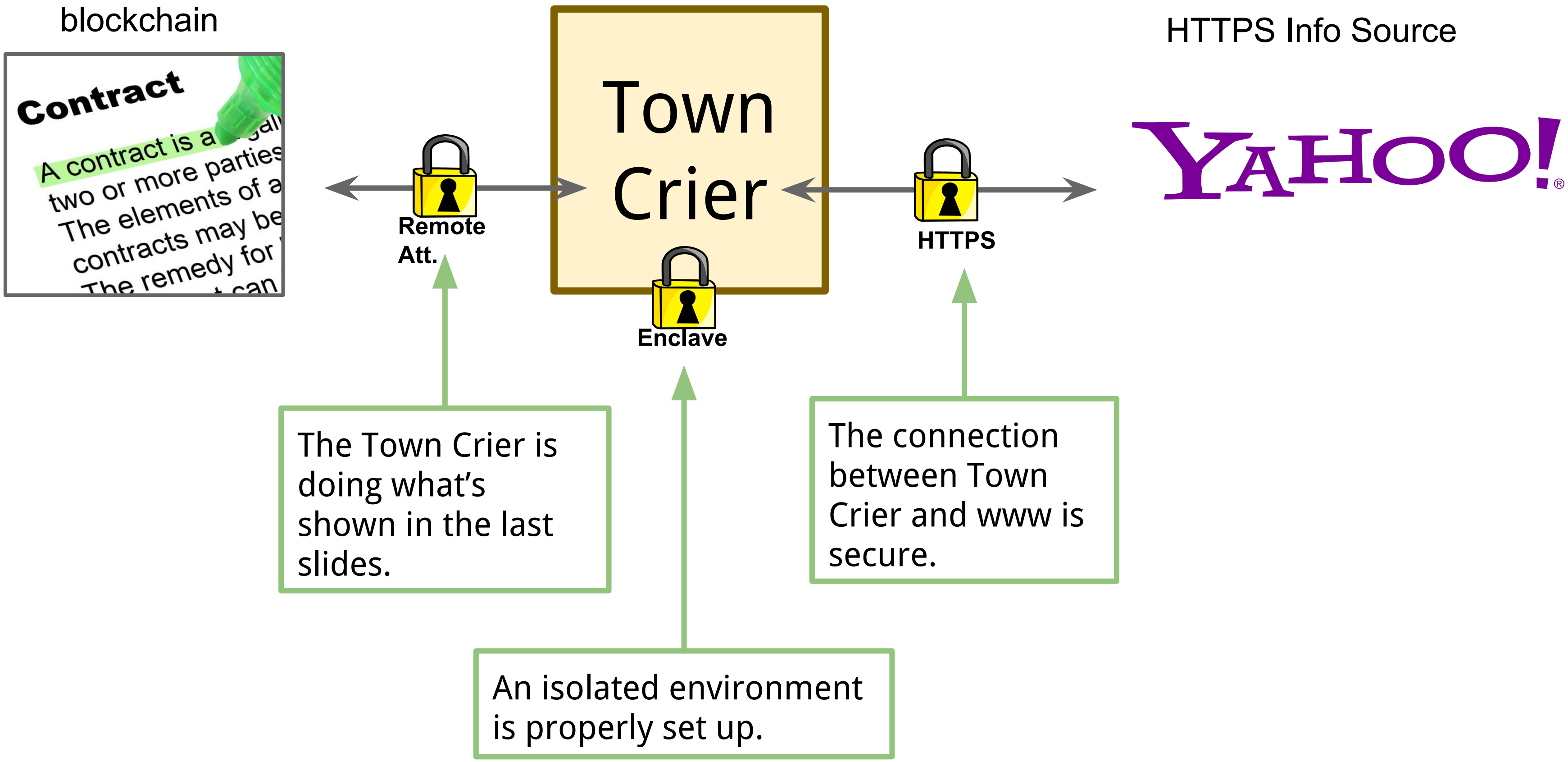
[9] Generate and sign the datagram. Send <data, signature> to the contract.

[10] **Verify** the signature

Use the data with confidence

...

Chain of Authenticity



blockchain

Town Crier

HTTPS Info Source

Remote Att.

Enclave

HTTPS

The Town Crier is doing what's shown in the last slides.

An isolated environment is properly set up.

The connection between Town Crier and www is secure.

Problem 1: HTTPS in an enclave

- Town Crier relies on HTTPS for authenticity
- But, enclave code can’t access the network card
- ??
- Solution: Put TLS layer in the enclave and TCP layer in the OS

Problem 2: Checking att in contracts?

- Too expensive
  - Code complexity
  - Gas expense
- Solution: piggyback it to Ethereum signature

Problem 3: Private / Custom Datagrams

- Example: the query includes a secret (e.g. API key to an online account)
- Solution: Encrypt the queries under TC’s public key

Questions?