Unifying Banks & Blockchains @ Coinbase

History of Coinbase

Bitcoin

Europe

Bitcoin Microservice

2012 2013 2014 2015 2016 2017

US Buy & Sell

Exchange (GDAX)

Ethereum

2 Trading Platforms

coinbase

3 Digital Currencies

6 Fiat Currencies

USD

EUR

GBP

SGD

CAD

AUD

7 Traditional Payment Integrations

PayPal

US Domestic Wires

3-D Secure Cards

32 Countries

4 Microservices

Knox (Private keys)

Macbeth (Ethereum)

Wallace (Bitcoin)

Iron Bank (US Banking)

1 Monolithic Rails App

What is Bitcoin?

Bitcoin is both:

1) a scarce digital resource
2) a protocol for transferring the resource over the Internet

US Banking System	Bitcoin
Bank accounts	Cryptographic addresses
ACH/Wire	Peer-to-peer protocol
Interbank settlement	Public transaction ledger
Issued by US government	Fixed issuance
3 business days	~30 minutes
Chargebacks	Irreversible payments

Overview

- How ACH & Bitcoin work
- Unified payments architecture
- How our ACH & Bitcoin services work

Automated Clearing House (ACH)

Originating Depository Financial Institution

ACH Operator (Federal Reserve)

Receiving Depository Financial Institution

Originator

Receiver

Automated Clearing House (ACH)

Originating Depository Financial Institution

ACH Operator (Federal Reserve)

Receiving Depository Financial Institution

Originator

Receiver

Automated Clearing House (ACH)

Originating Depository Financial Institution

ACH Operator (Federal Reserve)

Receiving Depository Financial Institution

Originator

Receiver

Automated Clearing House (ACH)

Originating Depository Financial Institution

ACH Operator (Federal Reserve)

Receiving Depository Financial Institution

Originator

Receiver

Automated Clearing House (ACH)

Originating Depository Financial Institution

ACH Operator (Federal Reserve)

Receiving Depository Financial Institution

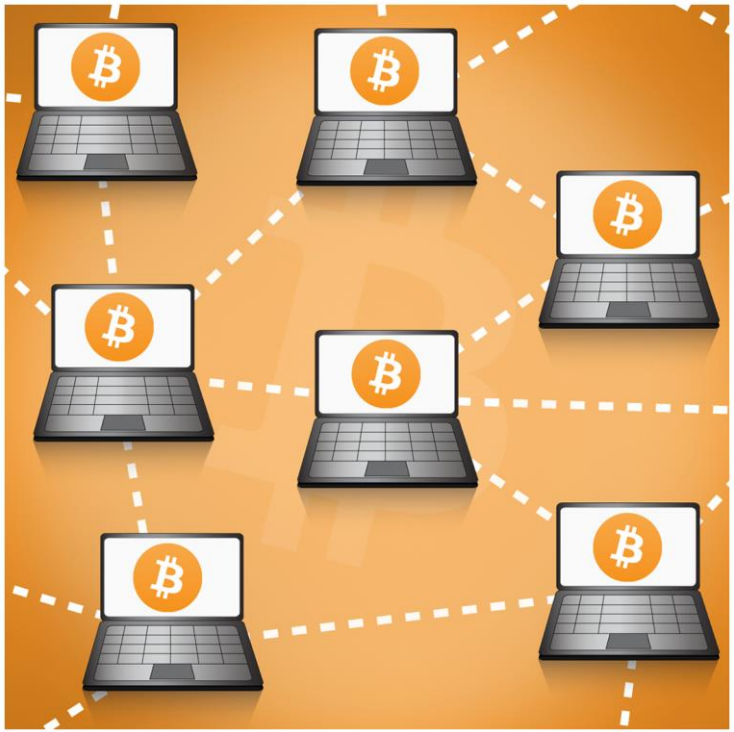
Originator

Receiver

ACH Returns

- Payments are returned if insufficient funds, account closed, unauthorized debit, etc.
- RDFI has 24 hours to return for insufficient funds
- Receiver has 60 days to issue a chargeback
- “No news is good news”

How Bitcoin Works



Cryptography Review

Digital signature schemes:

- Gen() => (Public key, Private key)
- Sign(Private key, Data) => Signature
- Verify(Public key, Data, Signature) => {True, False}

Collision-resistant one-way functions

- Hash(Data) => Fixed length binary string

Bits of Coin

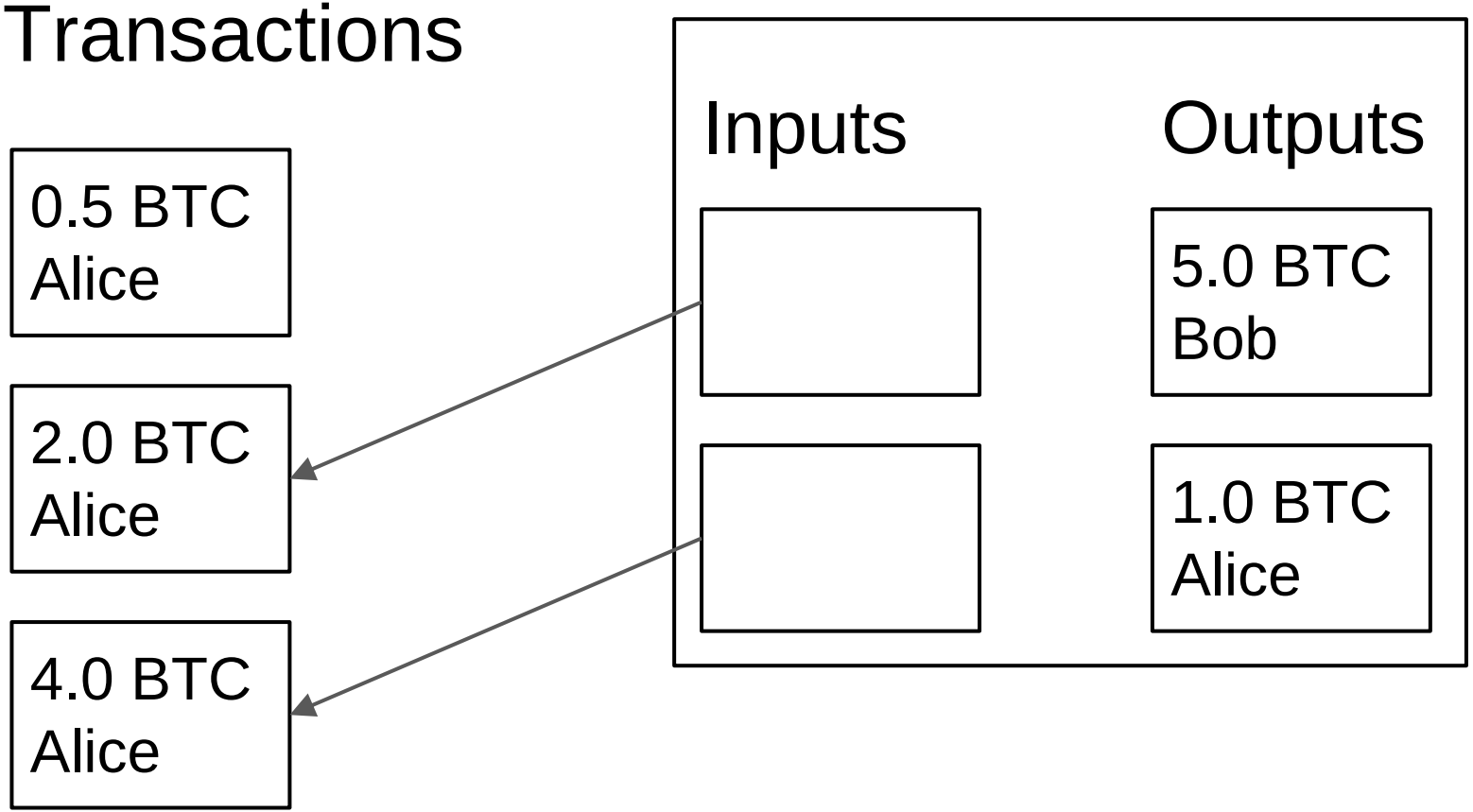
Transactions

0.5 BTC
Alice

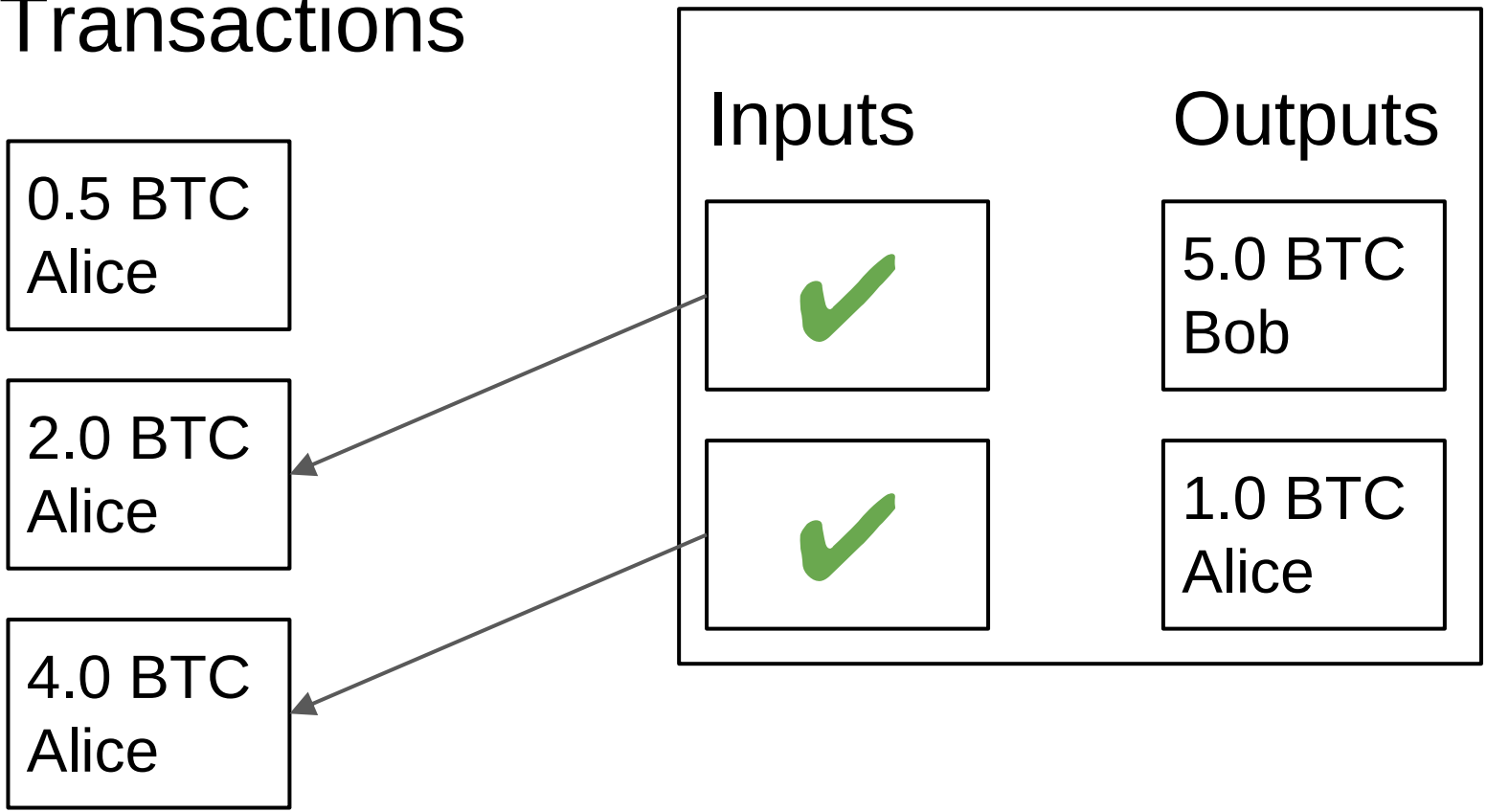
2.0 BTC
Alice

4.0 BTC
Alice

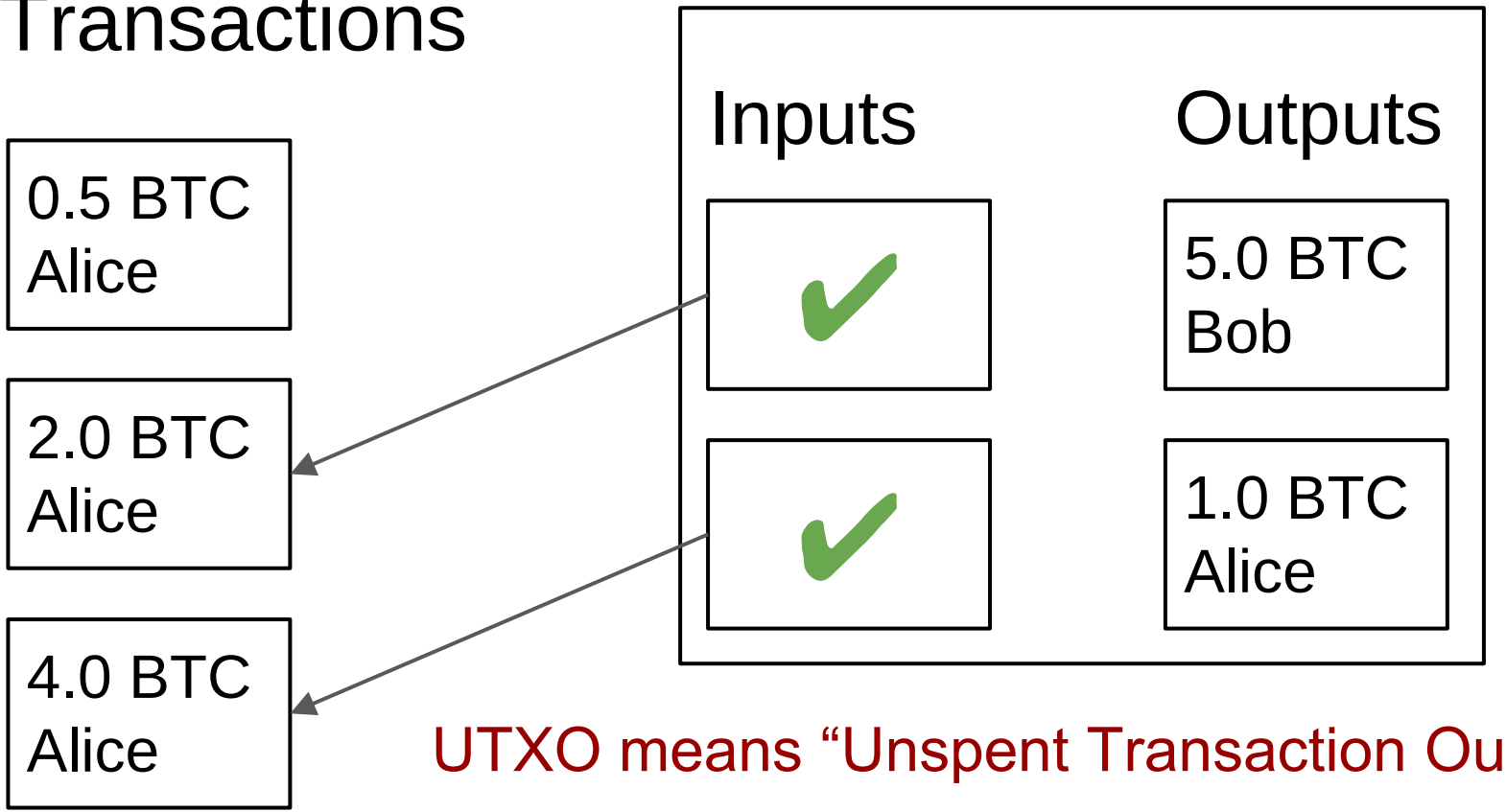
Transactions



Transactions



Transactions



UTXO means “Unspent Transaction Output”

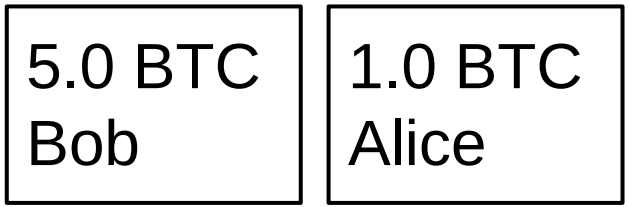
Public Ledger

Transaction #286

Public Ledger

Transaction #286

Transaction #287



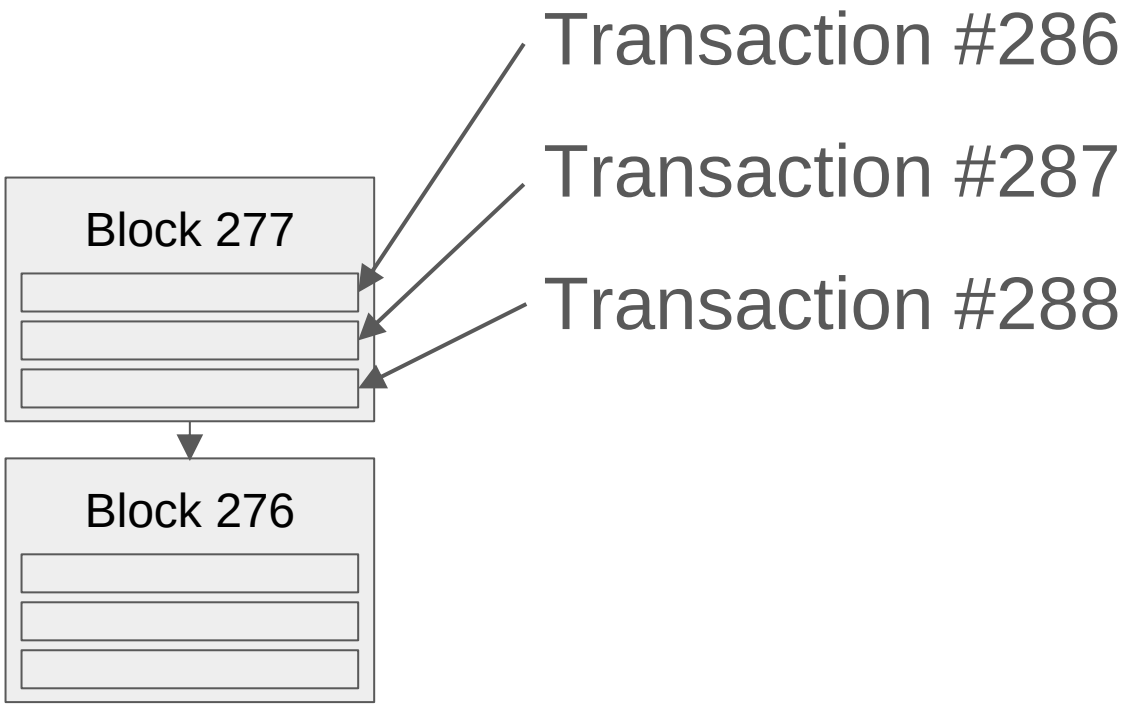
Public Ledger

Transaction #286

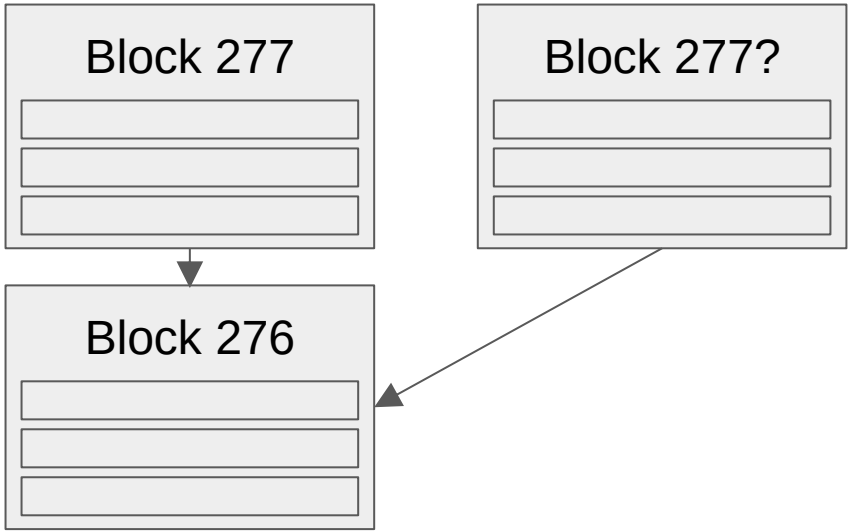
Transaction #287

Transaction #288

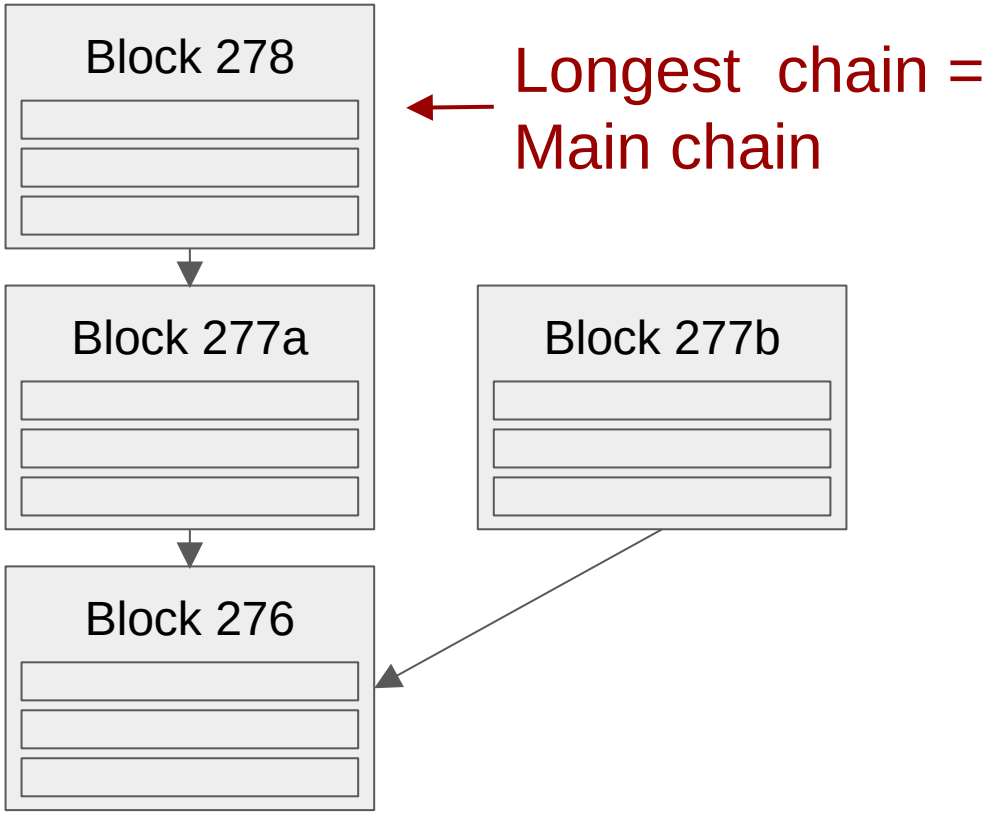
Blocks & Chains



Blocks & Chains



Blocks & Chains



Overview

- ~~How ACH & Bitcoin work~~
- Unified payments architecture
- How our ACH & Bitcoin services work

History of Coinbase

Bitcoin

Europe

Bitcoin Microservice

2012

2013

2014

2015

2016

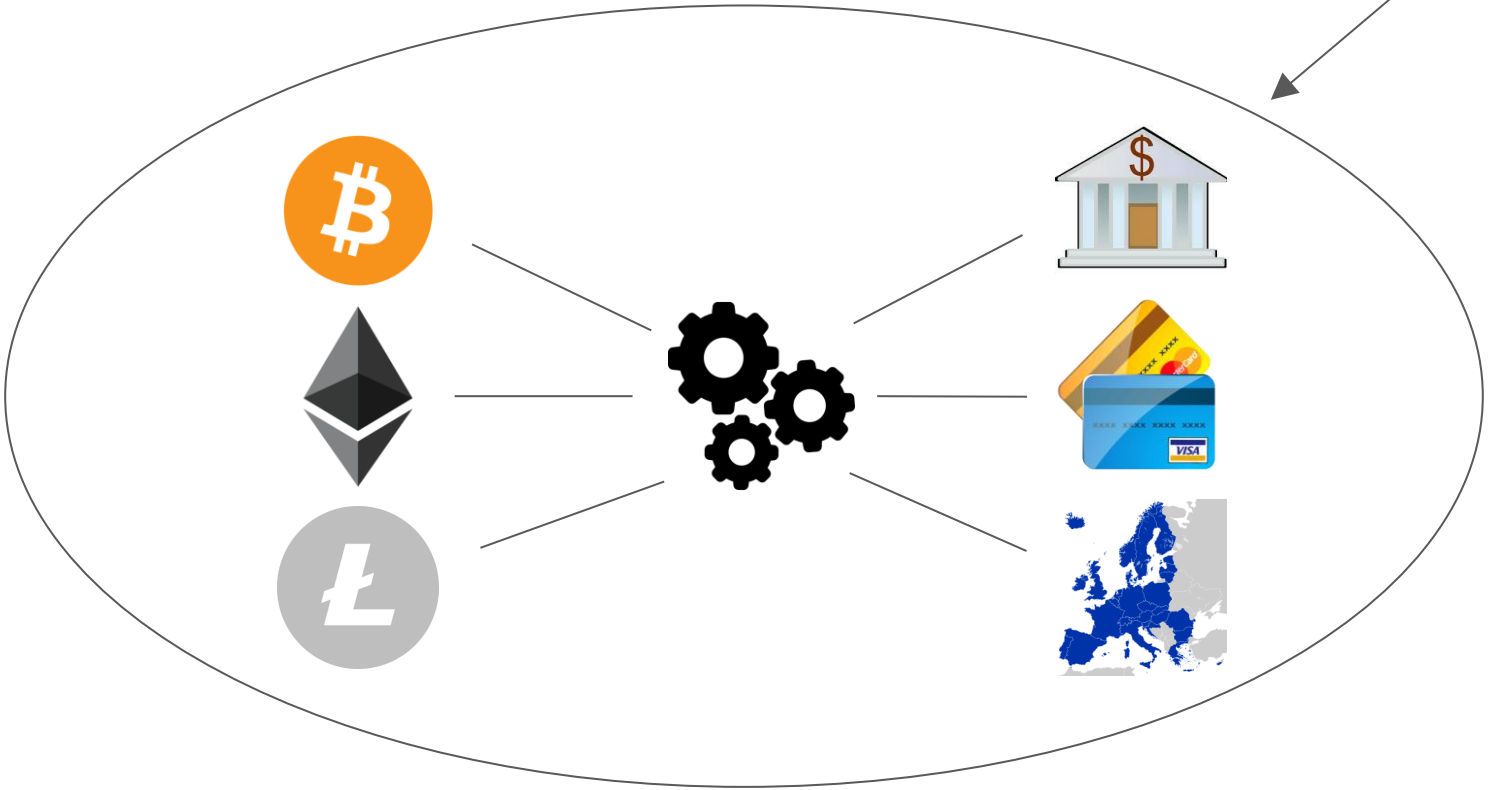
2017

US Buy & Sell

Exchange (GDAX)

Ethereum

A Not-So-Scalable Architecture

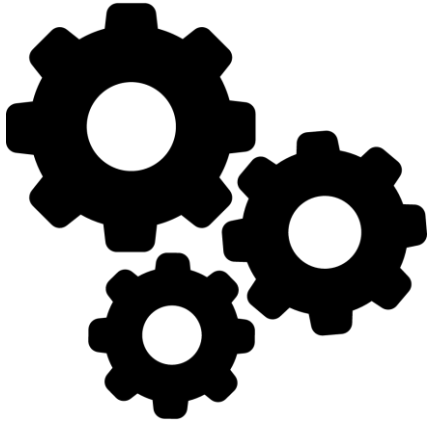


Core Transaction Processing

	Debit	**Credit**
Deposit	External account	Coinbase account
Withdrawal	Coinbase account	External account
Buy	Bank account	Coinbase crypto account
Sell	Coinbase crypto account	Bank account
Send	Coinbase account	Coinbase account

Transaction Processing Service

- Why is a payment made?
- Coordinates calls to payment services
- Ensures credits and debits balance out
- Buys, sells, deposits, withdrawals, sends

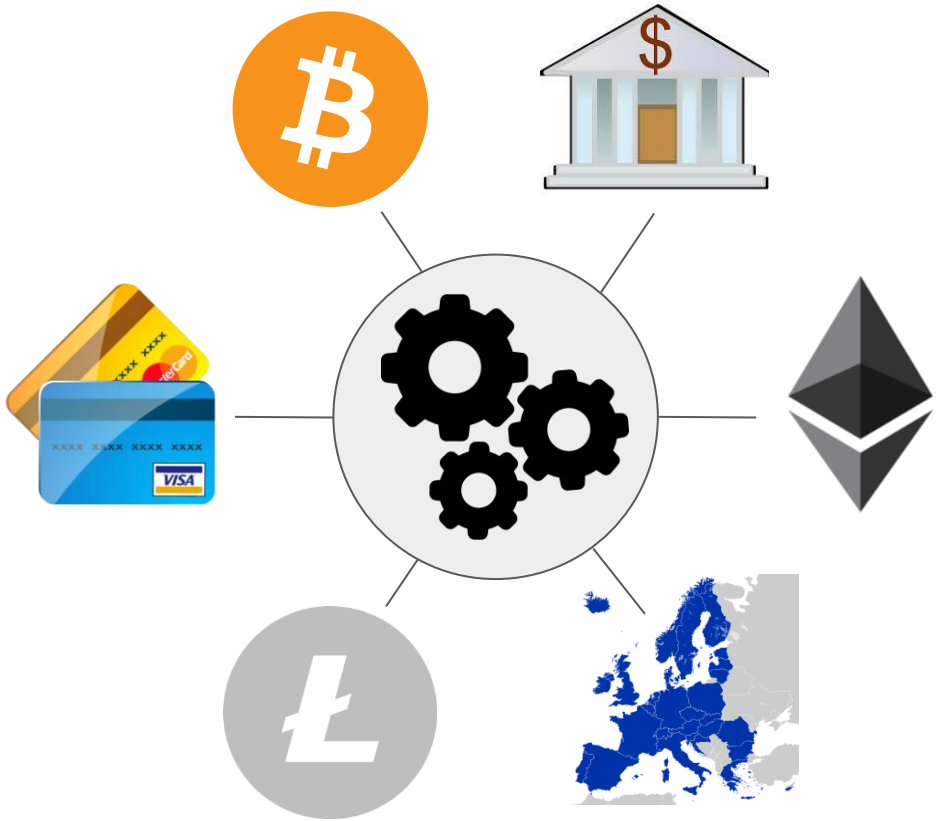


Payment Services

- How is a payment made?
- Can send and charge/receive money
- Encapsulates integration logic
- Implemented for both banks and blockchains




A Scalable Architecture

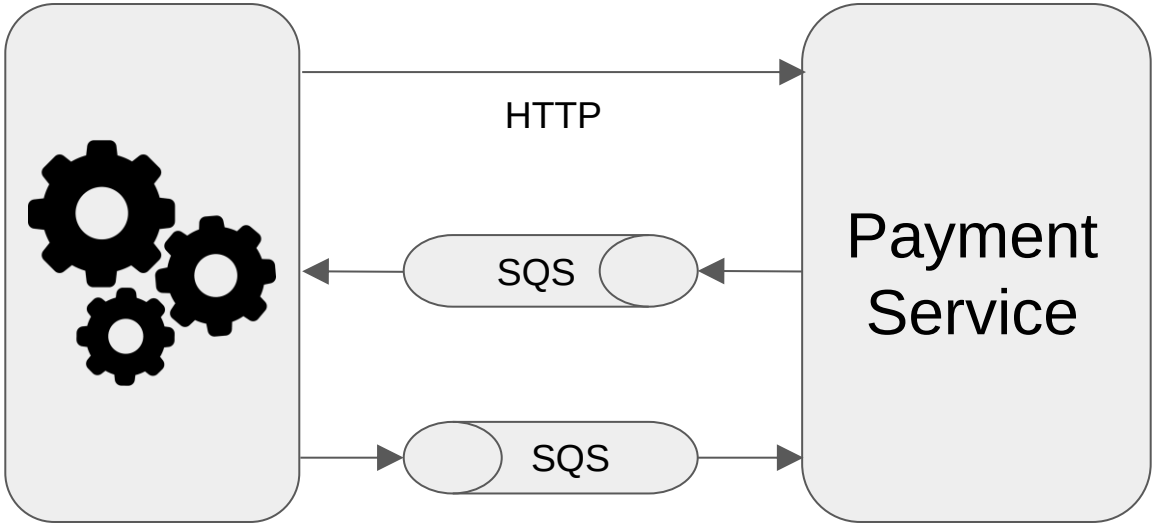


A Scalable Architecture

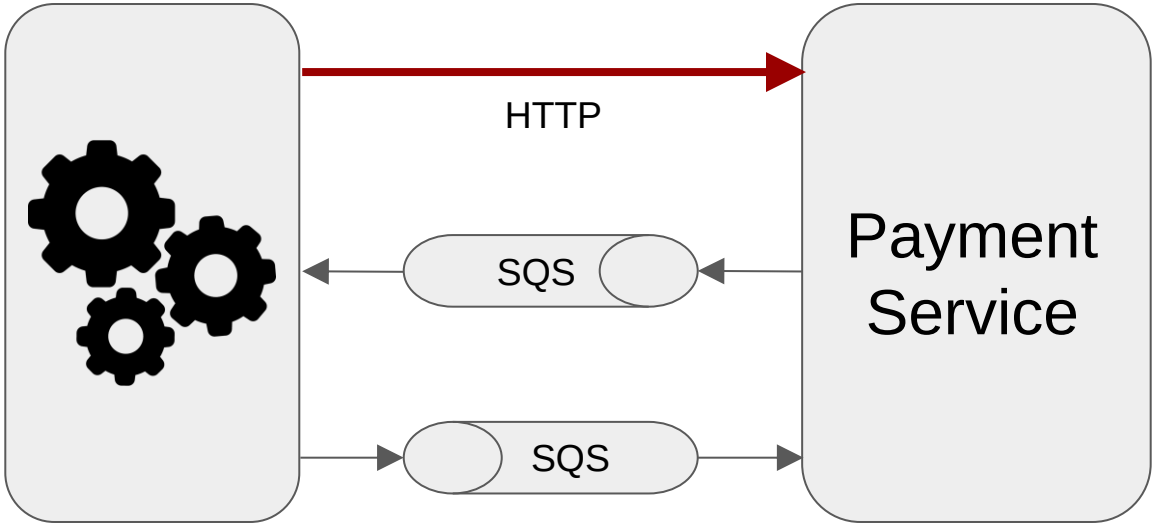
Universal Interface: Payment Structure


```
{
  "id": "21ee4091-ad9a-45b7-be49-6562ef19ea0e",
  "currency": "BTC",
  "amount": "-2.500000000",
  "fee": "0.000000000",
  "payment_method":
    "15pef9Cq8yd5a4b38DjKyKcT7R48VS4How",
  "account_id":
    "6ac6b0e1-8a2d-47d9-9f1e-bb3361b4f93e",
  "status": "completed"
}
```

Universal Interface: Microservice Protocol

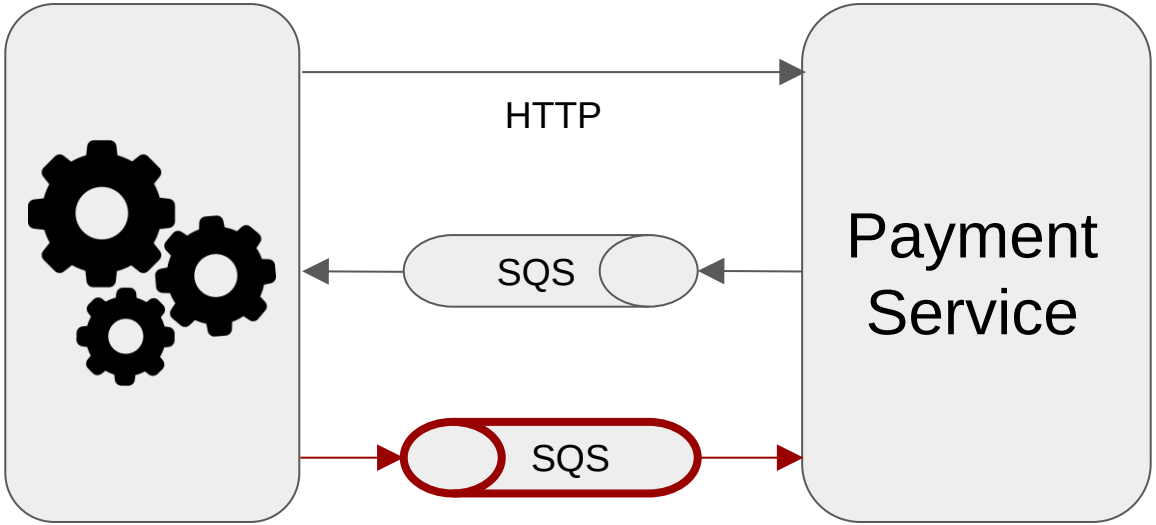


Universal Interface: Microservice Protocol



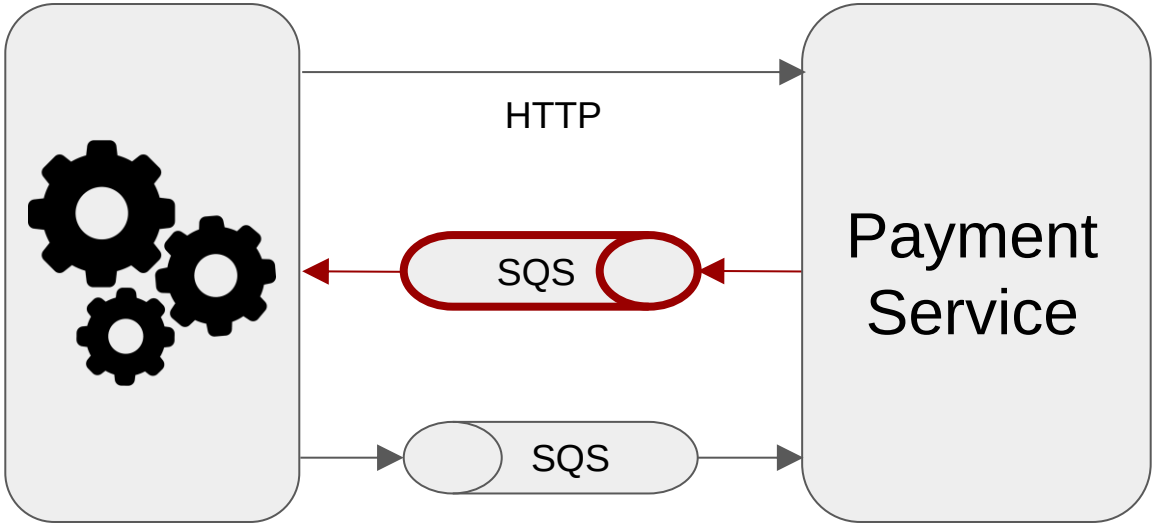
GET /payments/:id

Universal Interface: Microservice Protocol



create_payment(id, amount, currency, …)

Universal Interface: Microservice Protocol

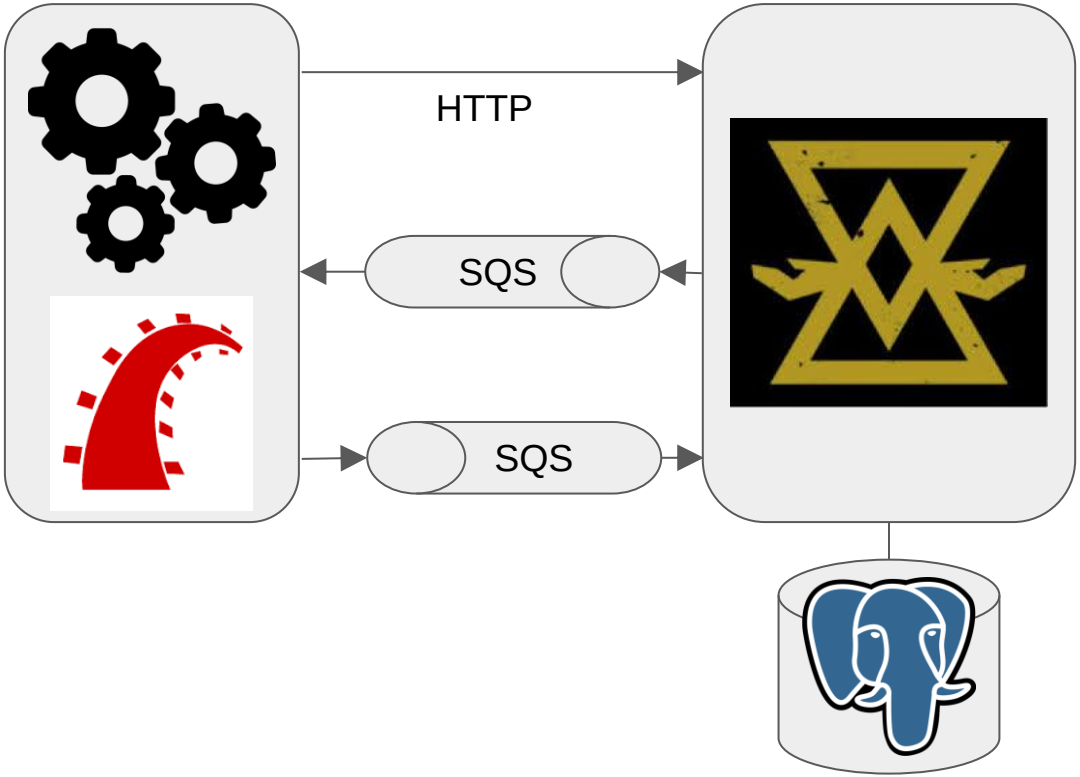


payment_update(id)

Overview

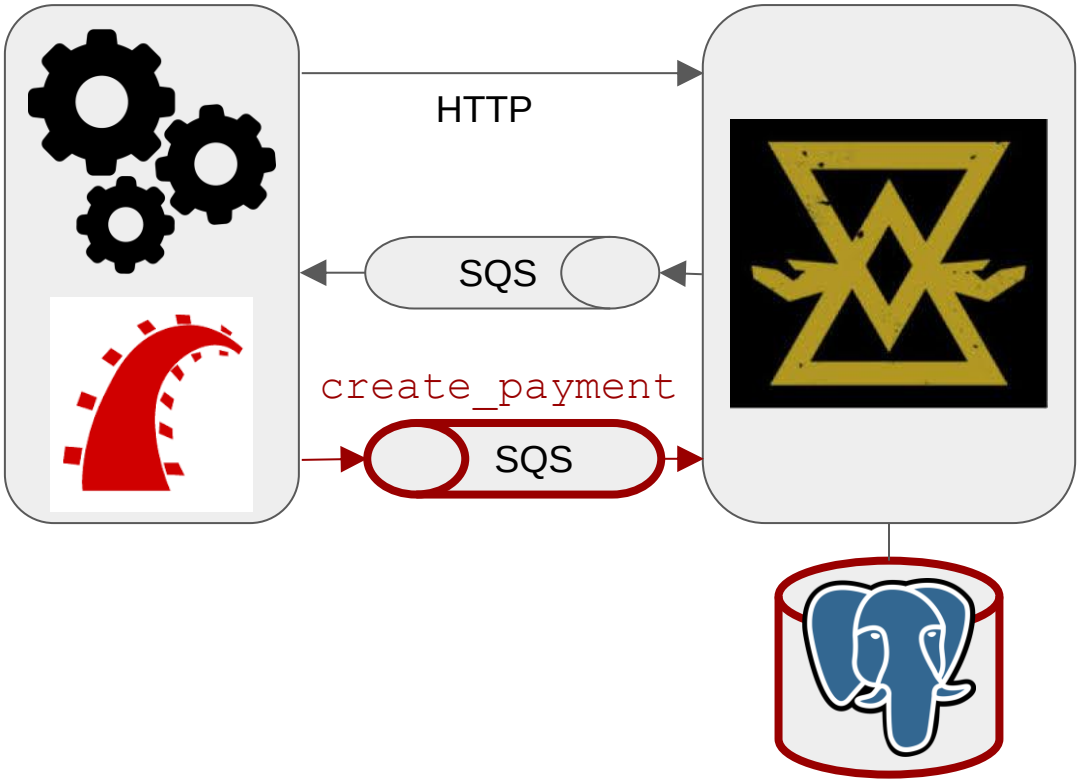
- ~~How ACH & Bitcoin work~~
- ~~Unified payments architecture~~
- How our ACH & Bitcoin services work

Iron Bank



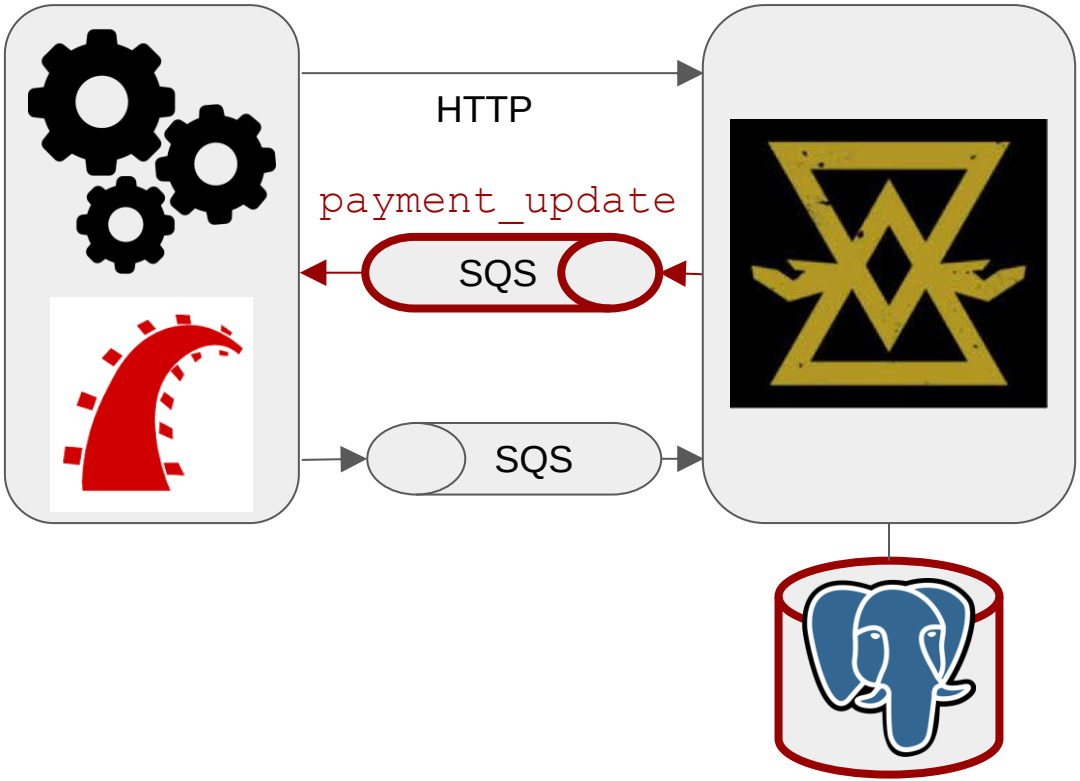
ODFI

Iron Bank



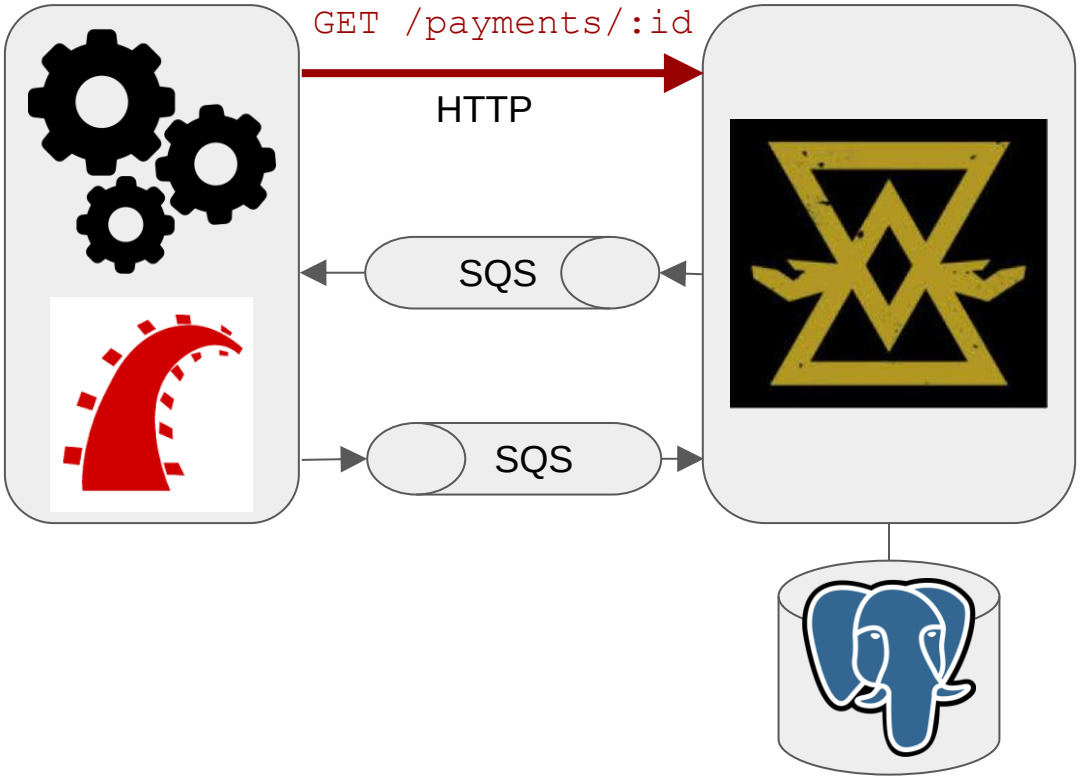
ODFI

Iron Bank



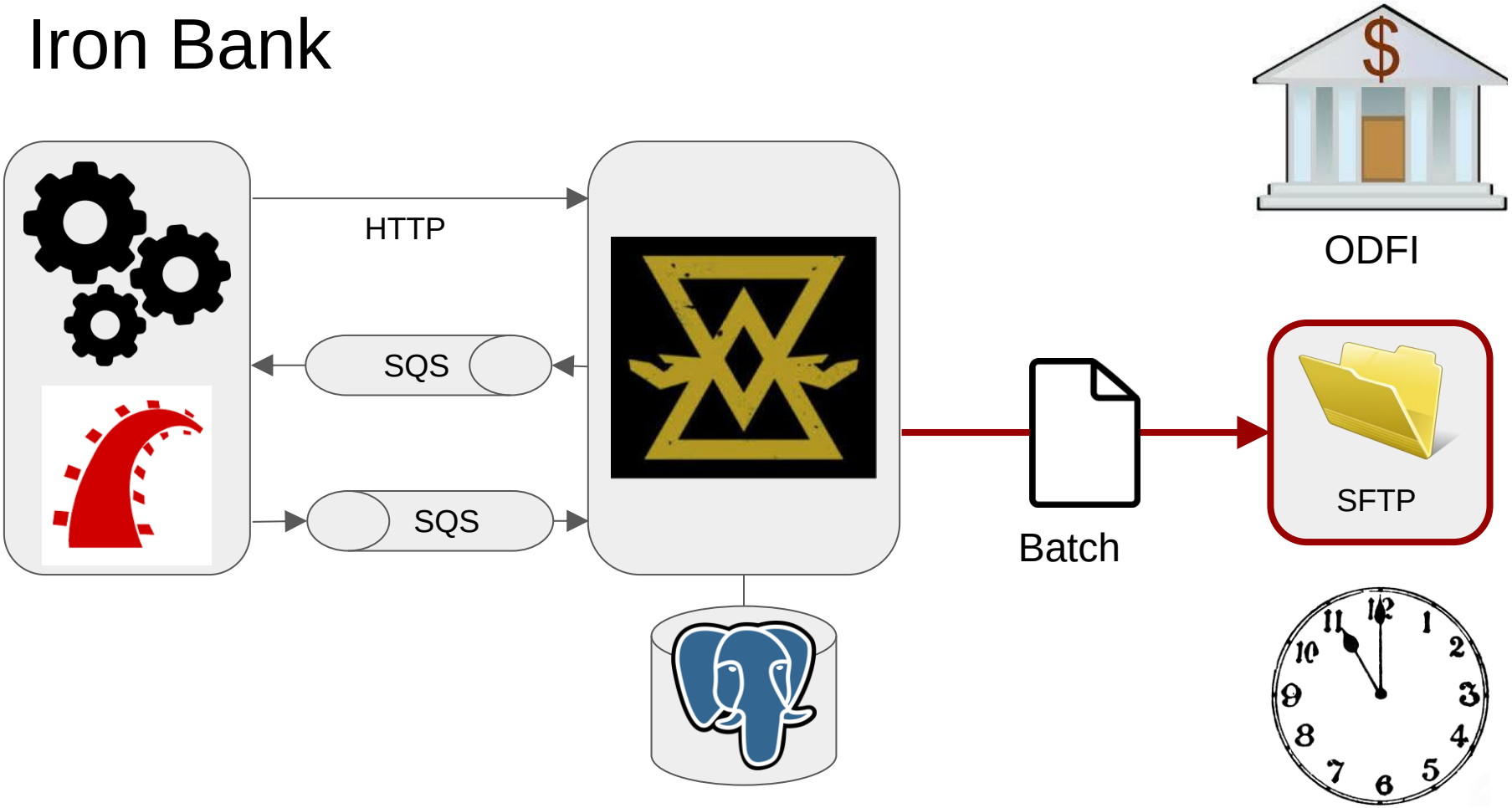
ODFI

Iron Bank

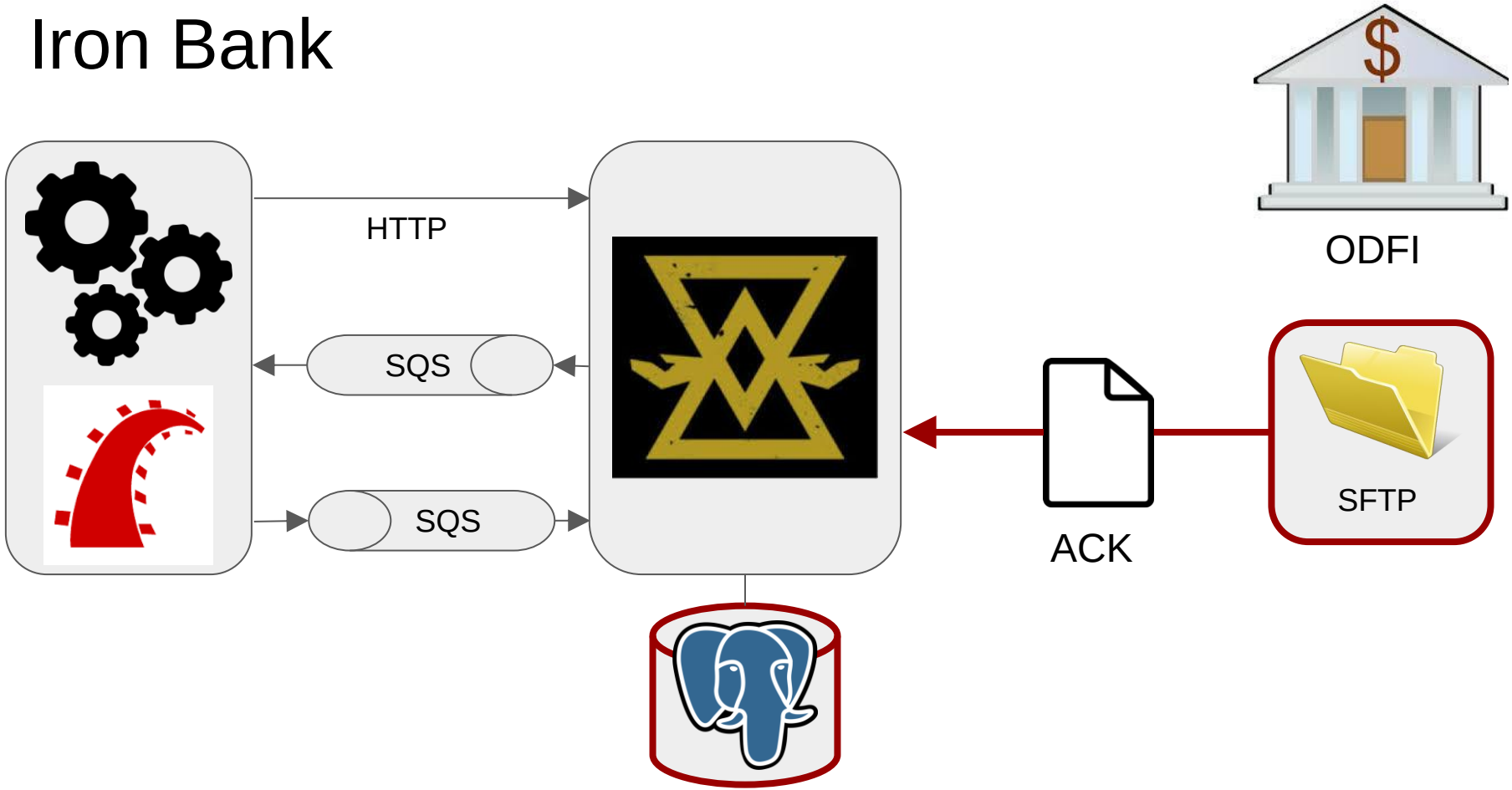


ODFI

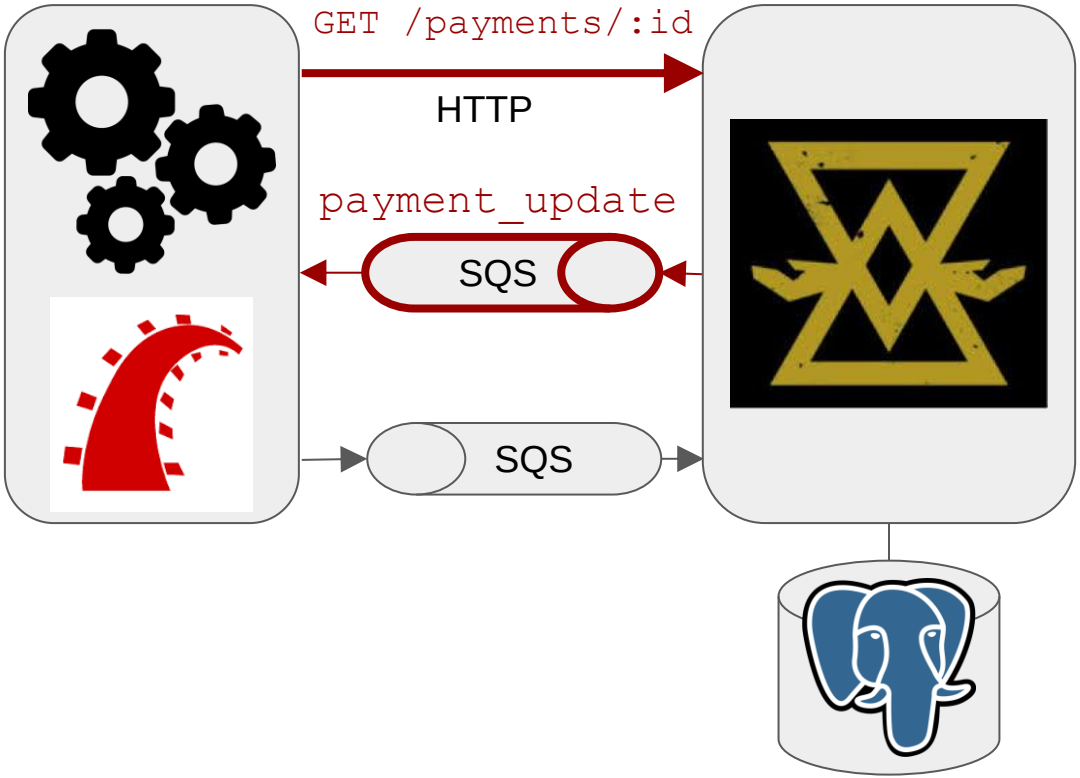
Iron Bank



Iron Bank

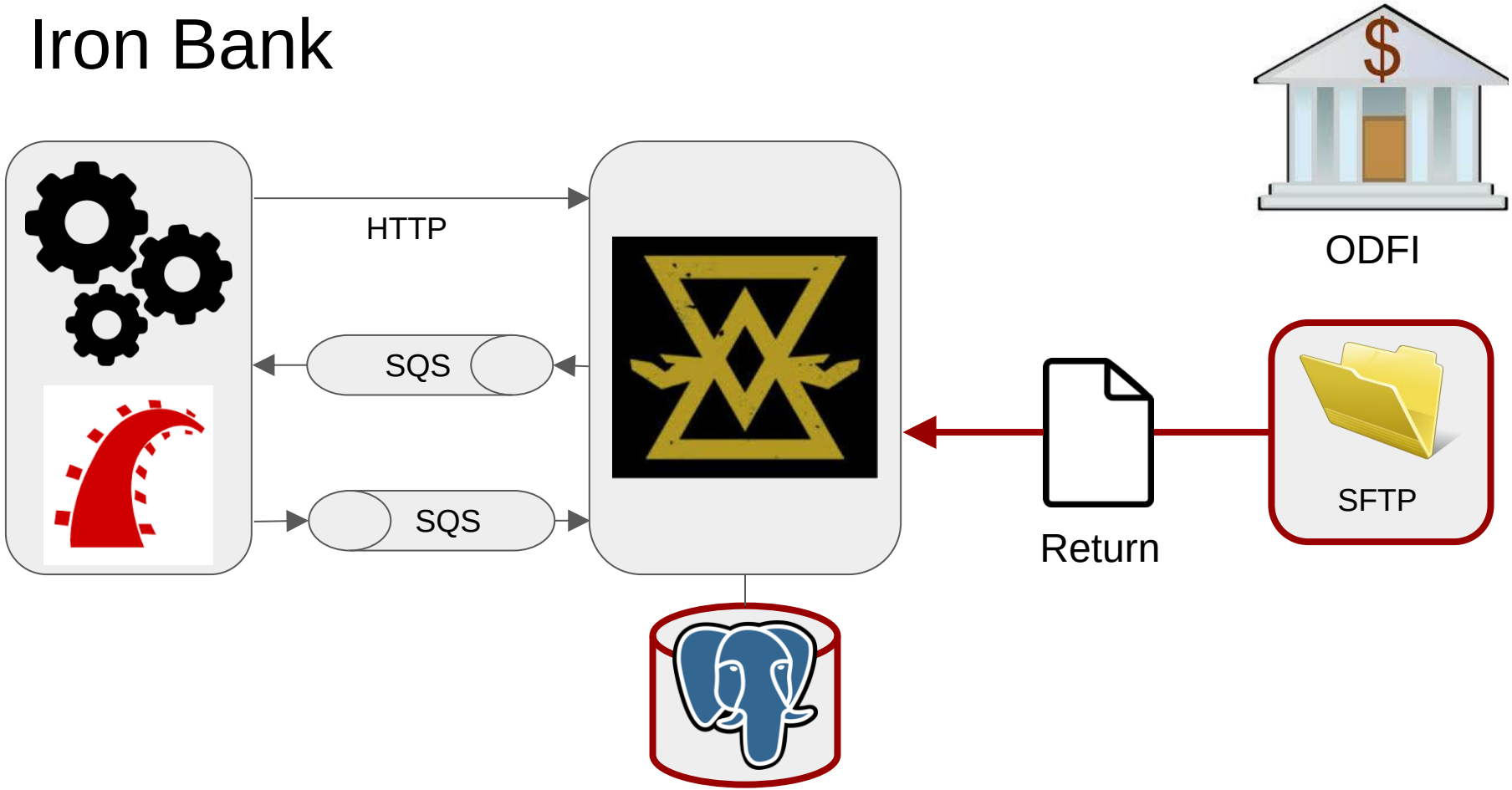


Iron Bank

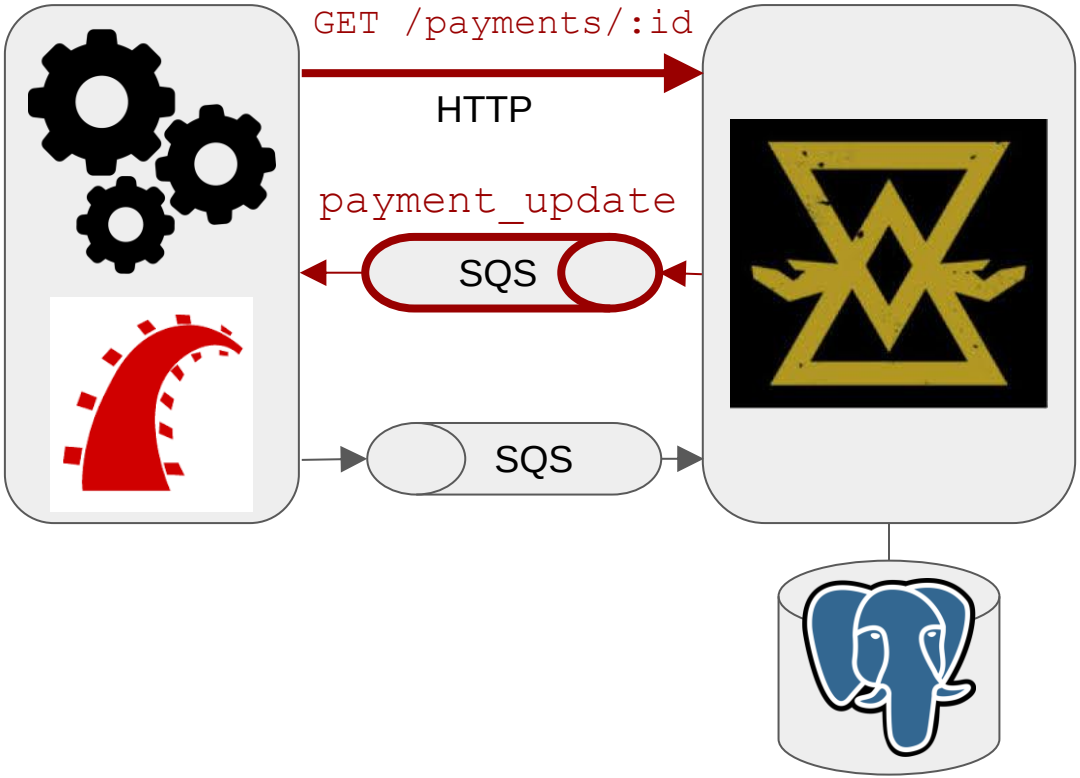


ODFI

Iron Bank



Iron Bank

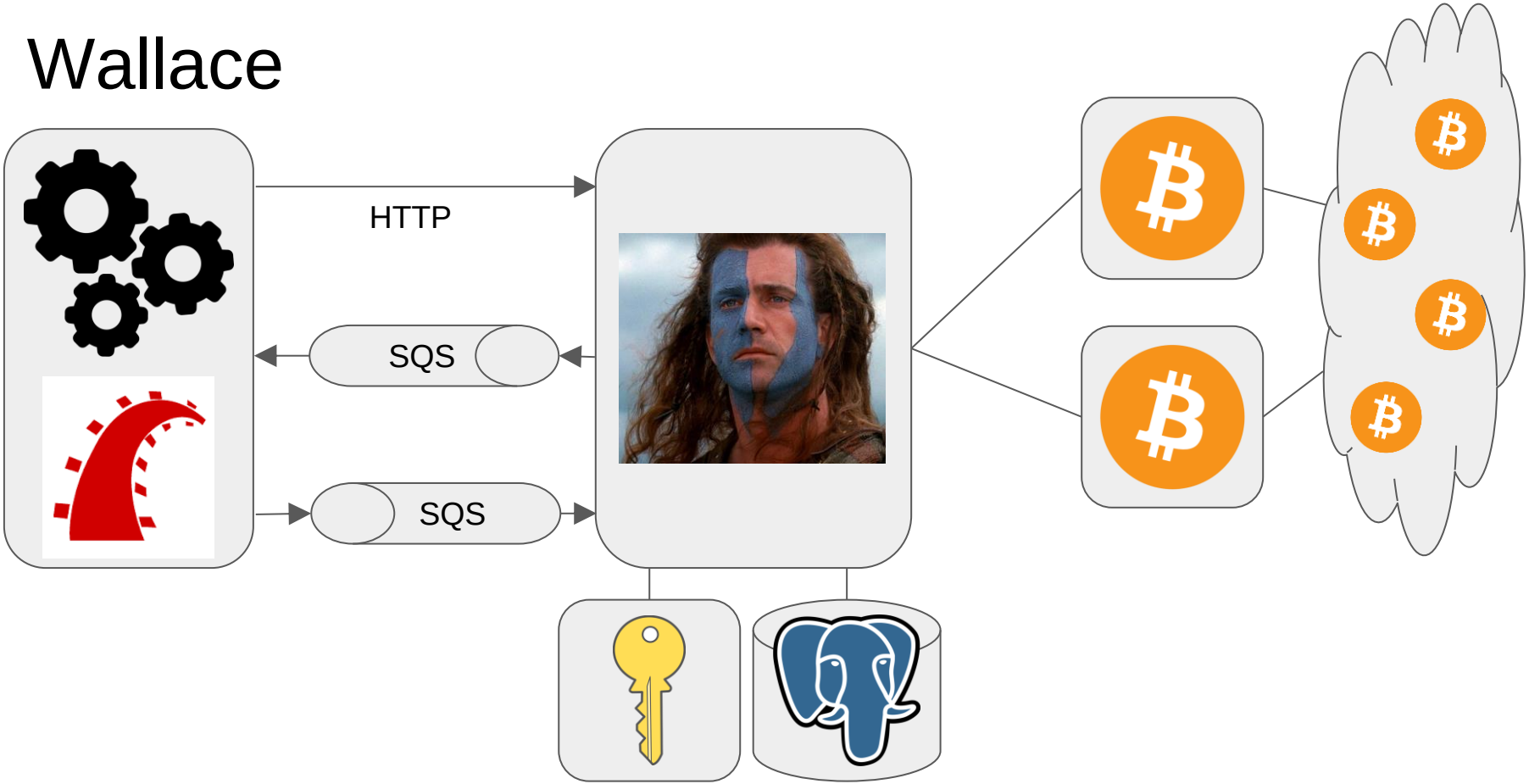


ODFI

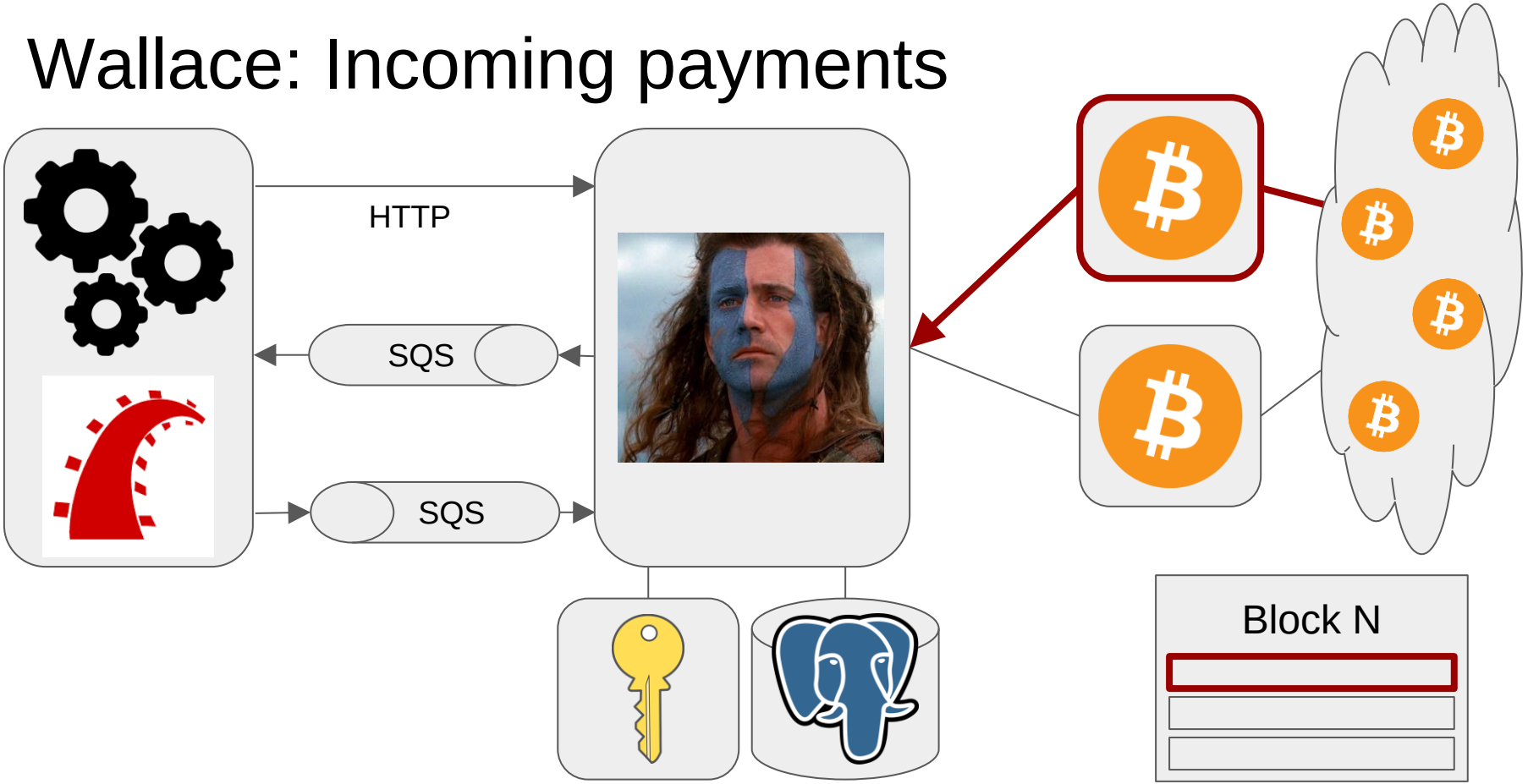
Iron Bank Details

- Multiple banks
- Quantity and volume limits per bank
- Web scrapers as alternative to FTP

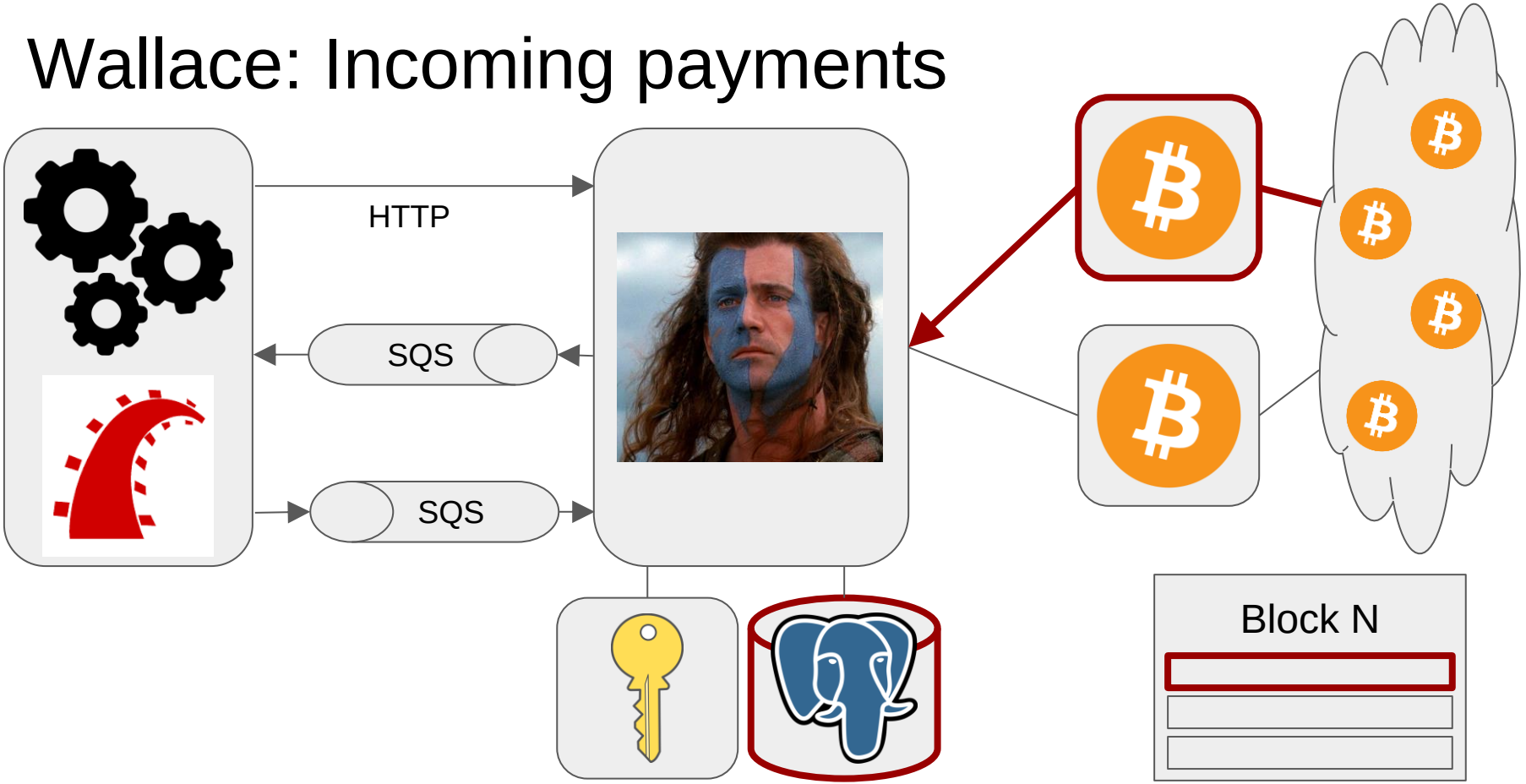
Wallace



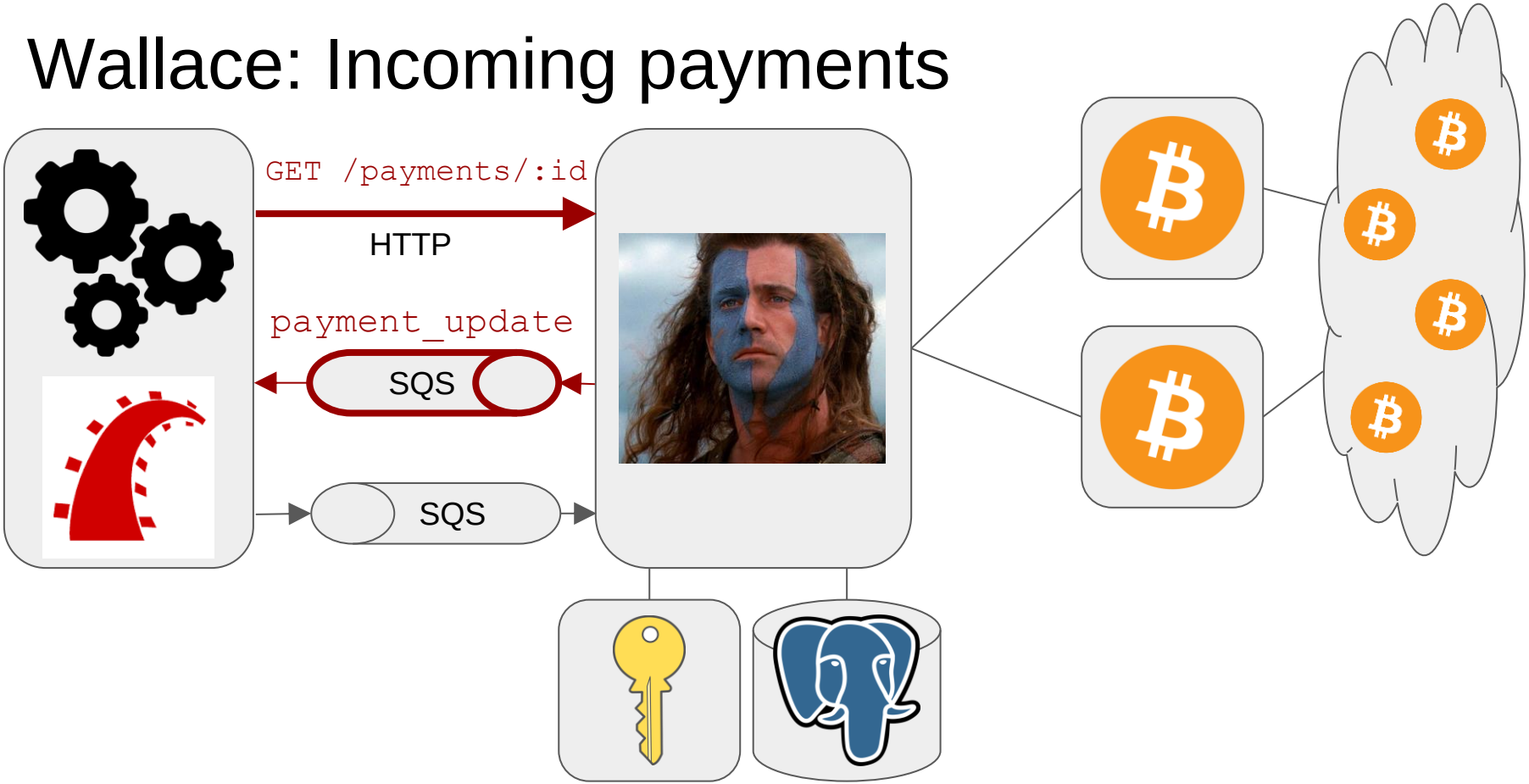
Wallace: Incoming payments



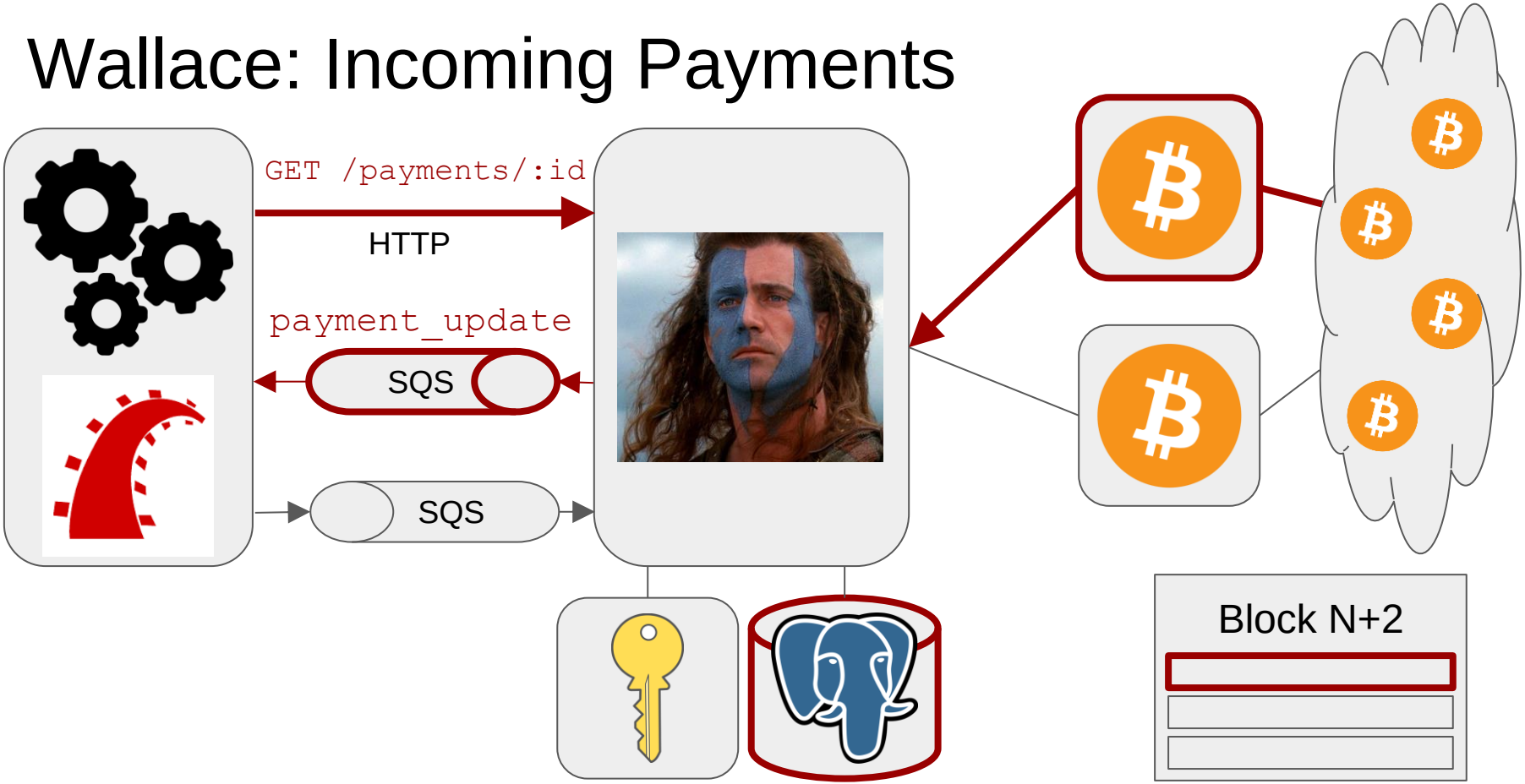
Wallace: Incoming payments



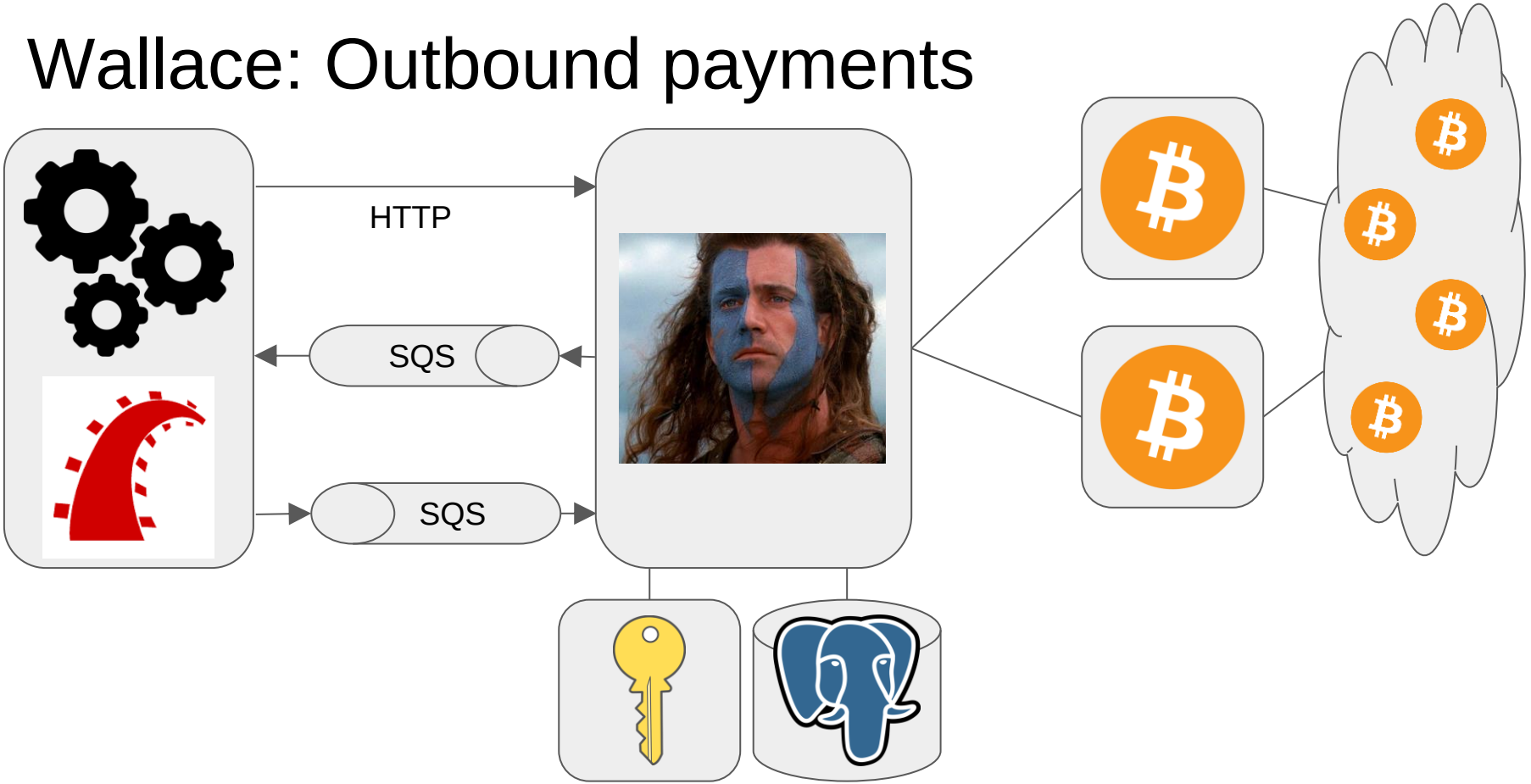
Wallace: Incoming payments



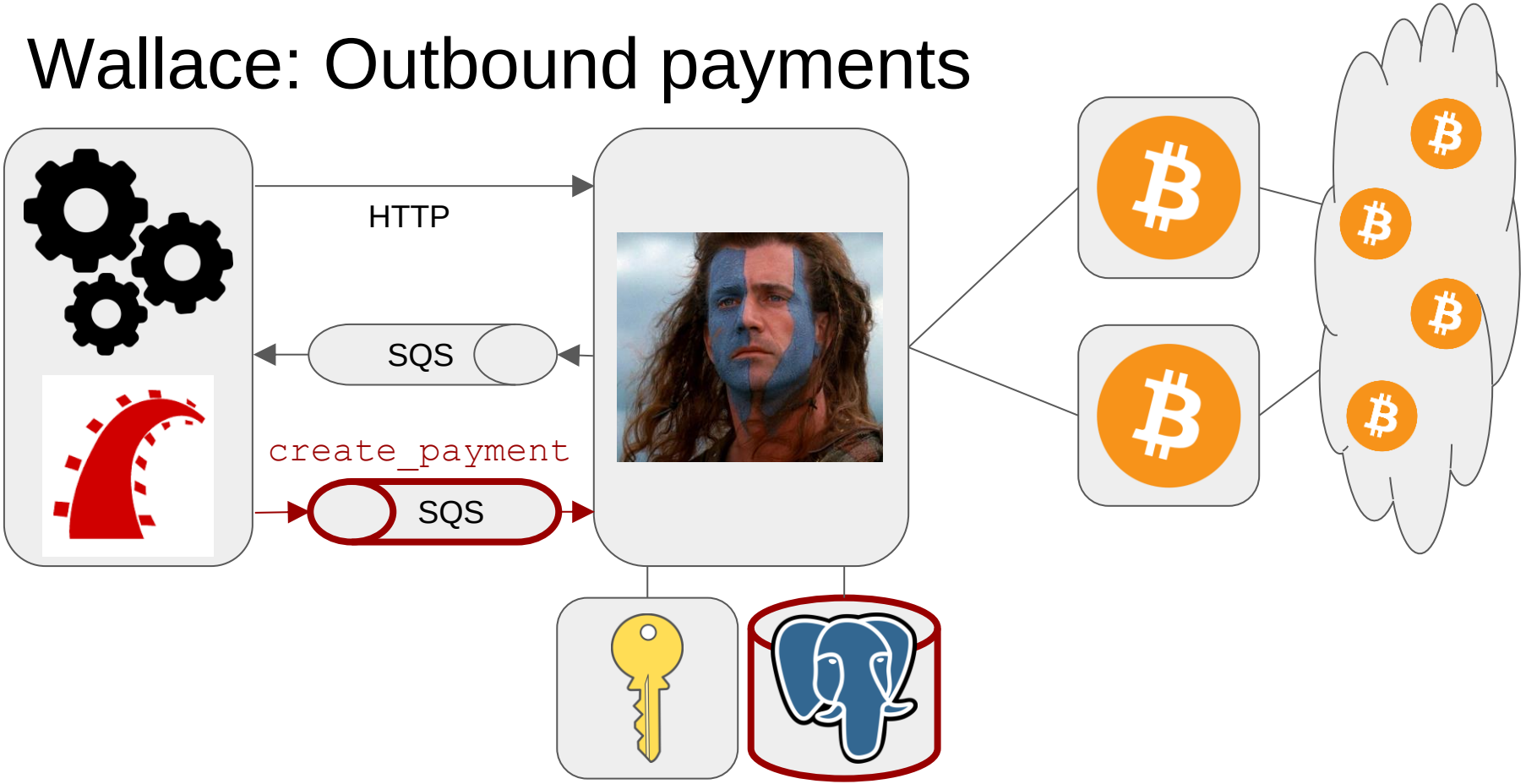
Wallace: Incoming Payments



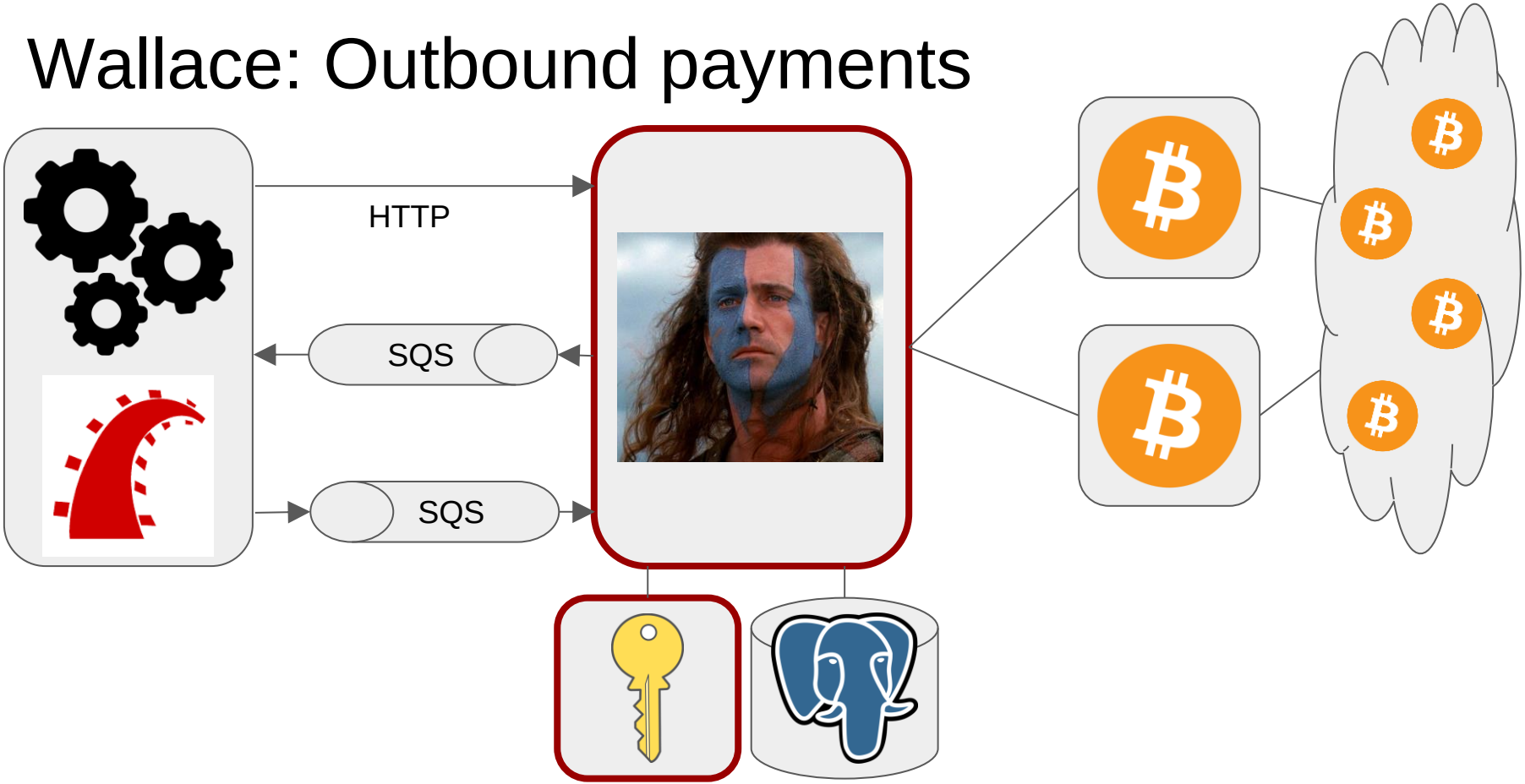
Wallace: Outbound payments



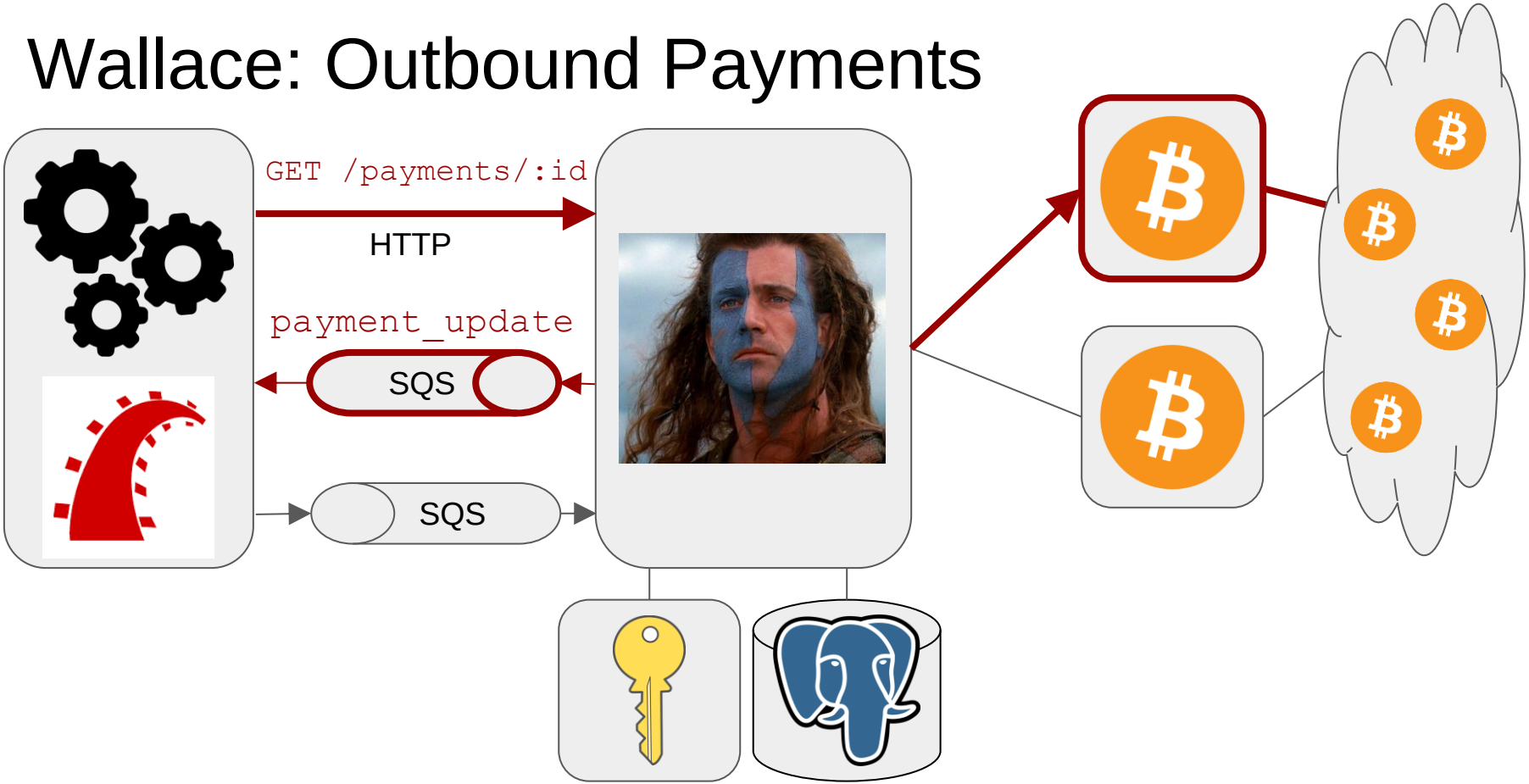
Wallace: Outbound payments



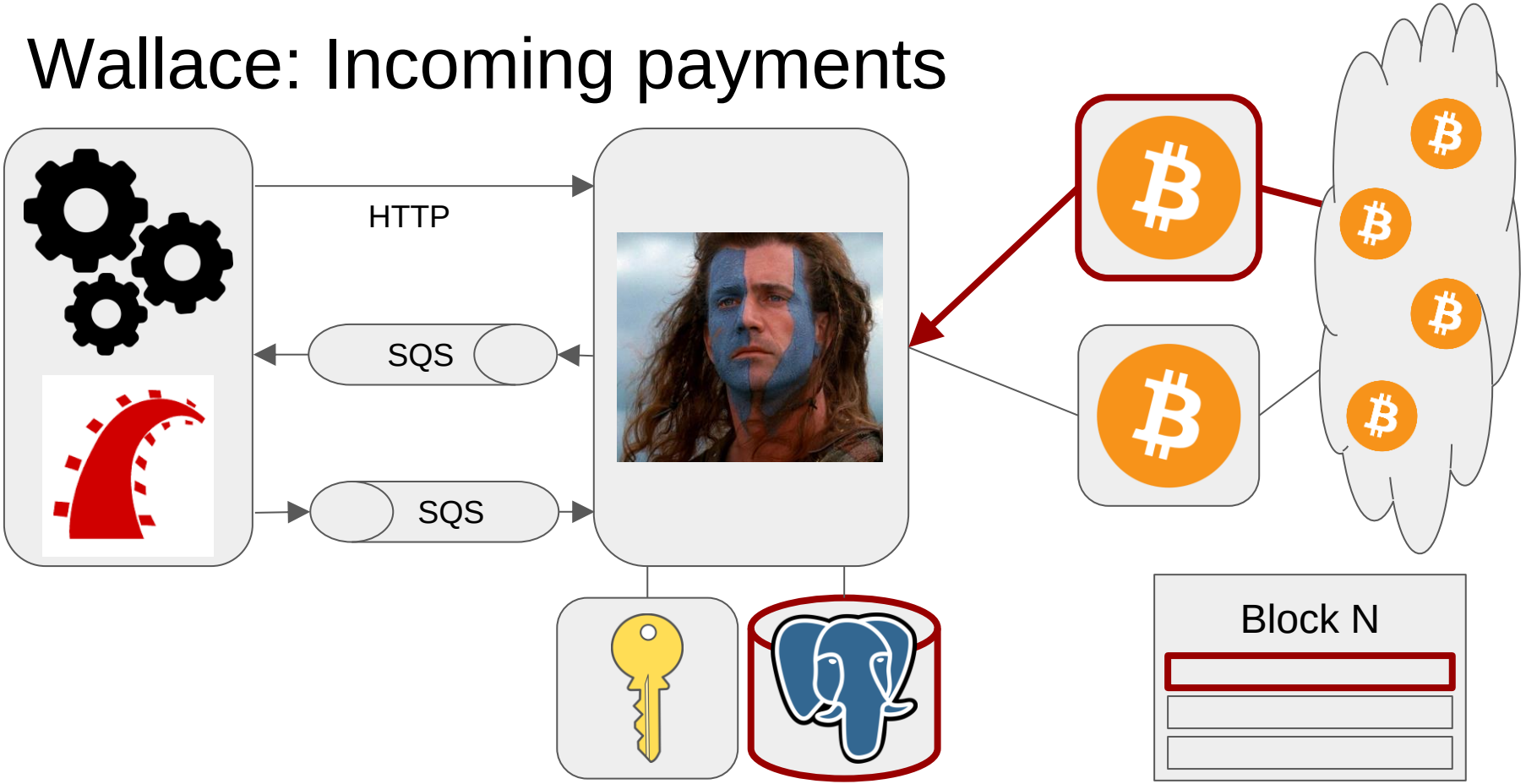
Wallace: Outbound payments



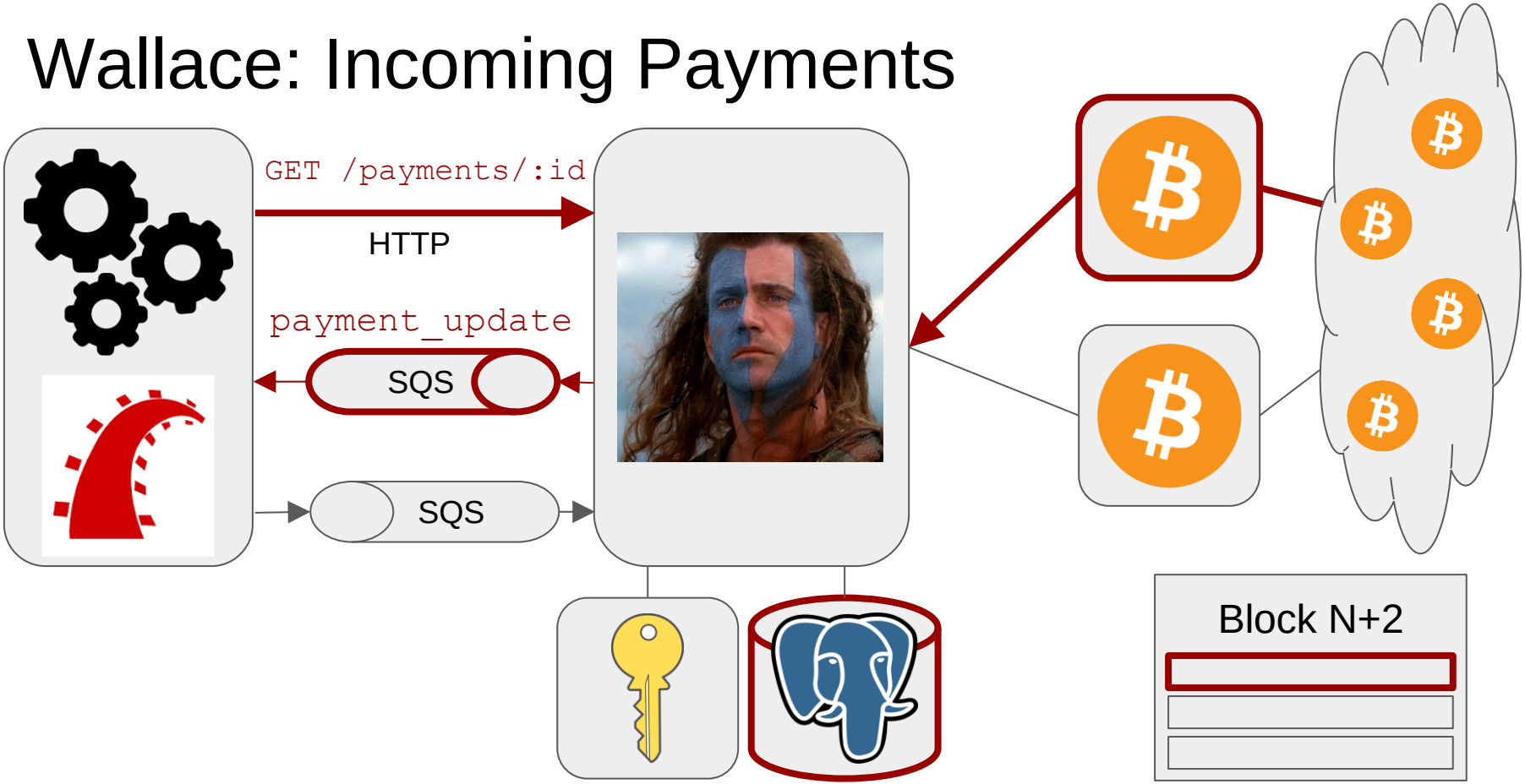
Wallace: Outbound Payments



Wallace: Incoming payments



Wallace: Incoming Payments



Wallace Details

- Transaction generation/UTXO selection
- Maintains separate pool of online & offline funds

Recap

- How blockchain integrations differ from banking integrations
- Evolution of Coinbase payments towards a unified architecture
- Polymorphic service interface using an abstraction of payments

Ongoing & Future Work

- Rearchitecture of existing integrations around new abstraction
- Migration of internal accounting to a microservice
- Dedicated microservice for core transaction processing

We would love your help :-)

Thanks for listening!

mailto:jimpo@coinbase.com