



Bitcoin Payment Integration

Karim Sultan, November 11 2017

CSI5380 - Professor Al Osman

Team: Seedy Music Club

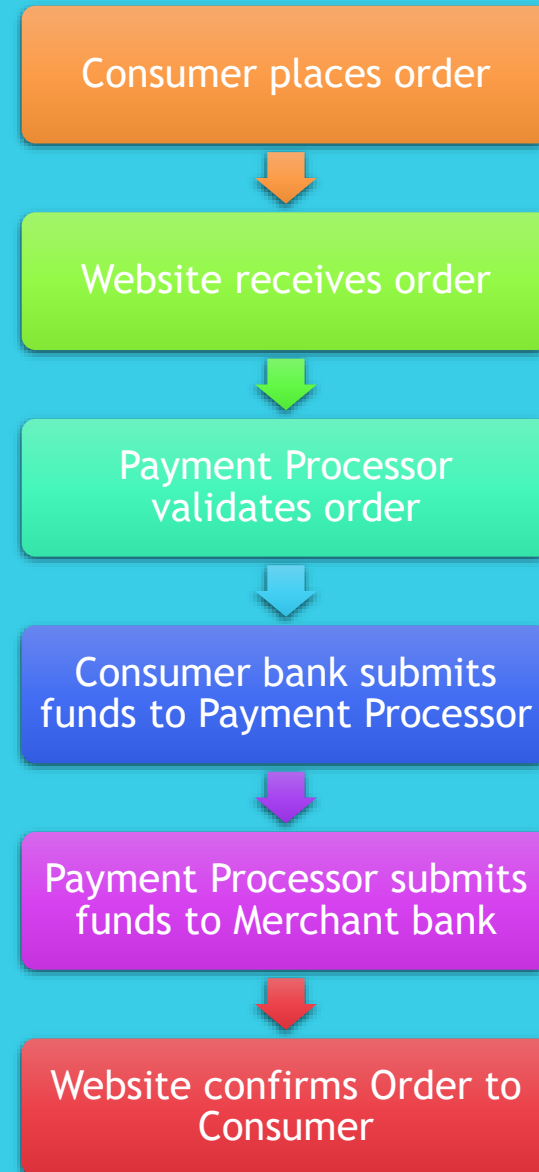
Goals

- **Prototype**
 - Modify ecom Site for Seedy Music Club
 - To accept Bitcoin as our payment methodology
 - To implement a Bitcoin invoice process via code
- **Research**
 - Each member must choose a work-packet to research
 - Must have at least 3 quality references, not counting Wikipedia references
- **Presentation**
 - Each member must prepare a 5 minute presentation of 1-5 slides
 - Each member must practice and present their slides

Key Terminology

- **Cryptocurrency** is digital cash secured via encryption
 - Obviously Bitcoin, but also Ethereum, and many more
- **Bitcoin** is the protocol and technology suite that runs the cryptocurrency
- **bitcoin** (lower case) is the “coin”
- **XBT** and **BTC** are the recognized exchange symbols
- **Blockchain** is the underlying tech; it is secure and decentralized and is sometimes called a “**distributed ledger**”
- A **transaction** is act of sending bitcoins to a recipient (purchase)
 - Can also be many other things, like escrow, group payments, etc... but 99% are purchases
- **Mining** is a complex, puzzle-solving race to find a **HASH** and **validate** the last 10 minutes of transactions

Review: Payment Gateway





Review: Bitcoin Gateway



Price Conversion

Convert Currency

- Currency must be converted from CDN (CAD) to BTC (XBT)

Real-time REST API calls:

- <https://api.coindesk.com/v1/bpi/currentprice/CAD.json>
- <https://api.cbix.ca/v1/convert?amount=19.99>

View it online:

- <http://json.parser.online.fr/>

XE Currency Converter: XBT to CAD




1 XBT = **9,162.94** CAD

Bitcoin ↔ Canadian Dollar
1 XBT = 9,162.94 CAD 1 CAD = 0.000109135 XBT
2017-11-15 18:43 UTC

Order Submission

- User clicks SUBMIT ORDER
 - Will say “Pay with Bitcoin”
- On order confirmation page
 - Given amount, address
 - See Overstock.com sample




EVGA GeForce 1050 Ti Graphic Card - 1.29 GHz Core - 1.39 GHz Boost CI on Overstock.com invoice ID 204130114.

\$235.82 USD
0.03291282 BTC

USE COINBASE WALLET

USE BITCOIN ADDRESS



Send exactly **0.03291282 BTC** to this address:

1KtzV72TU41SaC5tC4XvQGaeFDDiQdoBad

14:09

Enlarge

Waiting for Payment



Work Packets (Research / Slides, and Code)



#1: Cryptocurrencies

Definition: what is a cryptocurrency?

Compare and contrast 3-5 major cryptocurrencies

- ie: Bitcoin, Ethereum, Zcash, etc...

Acquisition: How do you purchase bitcoins?

Explain methods of getting bitcoins

- ie: Buy them at exchange, Bitcoin ATM, private peer transactions
- Compare and contrast 3 exchanges (fees, setup time, location)
- ie: CBIX, Coinbase, etc...

Legal: Regulatory Issues

Does Canada recognize bitcoin as money or investment?

Do Canadian merchants need to collect tax on BTC payments?

Other:

Current trends, statistics
interesting research results

#2: Wallets (aka e-wallet, digital wallet)

Definition: What is a wallet?

- Define general context (all cryptocurrencies) and specific (Bitcoin Wallet)
- Compare and contrast ~3 major Bitcoin wallets
 - ie: light/heavy, security, non-/deterministic, mobile/desktop, features

Storage: How do you store bitcoins?

- How are wallets secured?
- Compare hot and cold storage strategies (define, contrast)

Transactions: How do you send and receive bitcoins?

- Explain addresses and why we use multiple addresses
- Explain Bitcoin QR codes, what is encoded and how they work
 - Sample QR generator: <http://www.btcfrog.com/qr/>

Other:

- Trends and Statistics
- New research on wallets

#3: The Blockchain

Definition

What is a blockchain?
Why is there only one blockchain for Bitcoin, and how does it store balances?
What does it do? How does it store transactions? Why is it permanent?
How does it create trust?

Technical

Explain decentralized vs distributed
Consensus Algorithm: explain Proof of Work
Transactions: inputs vs outputs
Why can't you pull the plug on Bitcoin?

Mining

How does mining validate transactions? How long does it take?
How does mining work: puzzle-solving, hashes and difficulty
What is the economic incentive to mine?
Hardware required? What are mining pools?

#4: Bitcoin Payment Gateways

Definitions

- Payment Gateway, Payment Processor
- Settlement, Fee Structure

Process

- Visually contrast process of CC Payment Gateway vs Bitcoin Payment Gateway

Vendors

- Compare and contrast 3-5 top Bitcoin Payment Gateways
- Define: “Roll-your-own”

Integration

- Explain Vendor “commercial shopping cart integration”
- Explain Vendor APIs

#5: Bitcoin Assessment

Analysis: Analyse Bitcoin from a strategic perspective

Perform a SWOT Analysis on Bitcoin (shows current status)

Perform a Porter 5-Forces Analysis on Bitcoin (shows current strategy)

Market Maturity

Volatility: Show a price fluctuation graph, 3 year historical

Assess market maturity by comparing to CC gateway paradigm

Statistics: BTC adoption rate in ecom sites

Future

Outline key future trends / predictions

- ie: TPS increase, regulation, more players, ubiquitous cryptocurrency acceptance

Code 1/2: Bitcoin Integration - MVC Portion

View

- Add “My Account” to Navbar with “Order History”, “Logout” options
- New JSP: orderHistory.jsp to show list of all user’s orderId and status
- Bootstrap 4 - collapsible panel - to show selected order details

Controller

- Order Controller Servlet calls getOrderHistory() in Order Web Service
- Forwards to orderHistory.jsp
- Remove Auto-Denial: no more dropping every 5th order

Model

- New method listOrdersByUserId(int Id)
- Order status now: OPEN, PENDING, PAID, DECLINED, *SHIPPED*

Code 2/2 Bitcoin Integration - Confirm Order

- Order Confirmation now must:
 - Convert shopping cart total from CAD to BTC
 - Generate a new private/public key pair for the order, updated DB
 - Generate a QR code using public key, BTC price
- “Lazy” status update
 - DAO will do the following for any order in a pending state, when it is requested:
 - Check for an approved transaction in the blockchain;
 - Update order status to PAID if found;
 - If 24 hours have passed and no approval, set order status to DECLINED