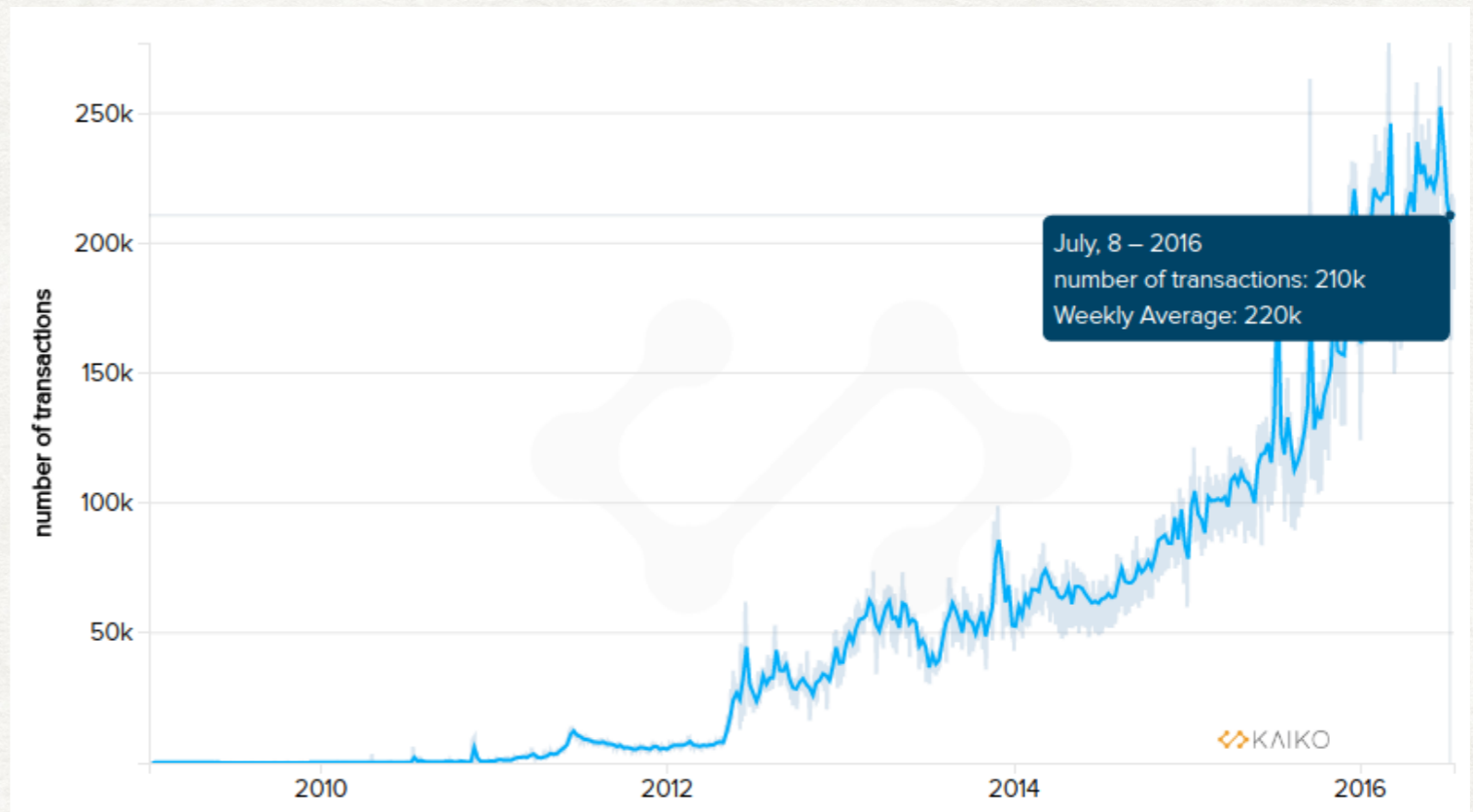# BITCOIN
YET ANOTHER INTRODUCTION

- The first and most popular cryptocurrency since 2009

- Market cap of nearly 11 billion USD

- July 2016 stats (per day):

  - 210,000 transactions
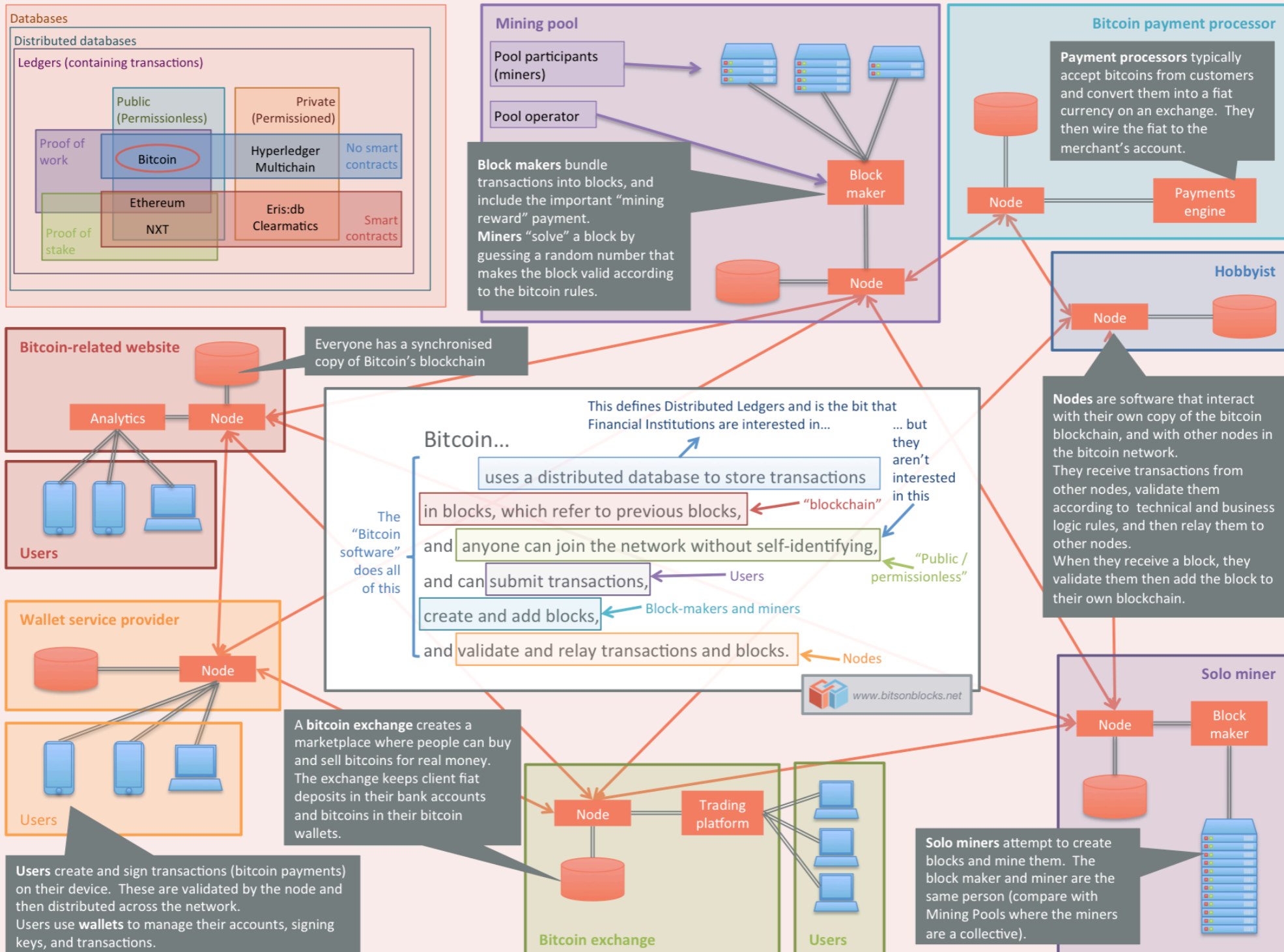
  - 360 K BTC = 200 Million USD

BITCOIN

YET ANOTHER INTRODUCTION

Bitcoin's network in one page, from *www.bitsonblocks.net*

Databases

Distributed databases

Ledgers (containing transactions)

	Public (Permissionless)	Private (Permissioned)	
Proof of work	Bitcoin	Hyperledger Multichain	No smart contracts
Proof of stake	Ethereum	Eris:db Clearmatics	Smart contracts
	NXT		

Mining pool

Pool participants (miners)

Pool operator

Block maker

Node

Block makers bundle transactions into blocks, and include the important "mining reward" payment.
Miners "solve" a block by guessing a random number that makes the block valid according to the bitcoin rules.

Bitcoin payment processor

Payment processors typically accept bitcoins from customers and convert them into a fiat currency on an exchange. They then wire the fiat to the merchant's account.

Node — Payments engine

Everyone has a synchronised copy of Bitcoin's blockchain

Hobbyist

Node

Nodes are software that interact with their own copy of the bitcoin blockchain, and with other nodes in the bitcoin network.
They receive transactions from other nodes, validate them according to technical and business logic rules, and then relay them to other nodes.
When they receive a block, they validate them then add the block to their own blockchain.

Bitcoin-related website

Analytics — Node

Users

Bitcoin…

This defines Distributed Ledgers and is the bit that Financial Institutions are interested in…

… but they aren't interested in this

The "Bitcoin software" does all of this

uses a distributed database to store transactions

in blocks, which refer to previous blocks, — "blockchain"

and anyone can join the network without self-identifying, — "Public / permissionless"

and can submit transactions, — Users

create and add blocks, — Block-makers and miners

and validate and relay transactions and blocks. — Nodes

www.bitsonblocks.net

Wallet service provider

Node

Users

A **bitcoin exchange** creates a marketplace where people can buy and sell bitcoins for real money. The exchange keeps client fiat deposits in their bank accounts and bitcoins in their bitcoin wallets.

Users create and sign transactions (bitcoin payments) on their device. These are validated by the node and then distributed across the network.
Users use **wallets** to manage their accounts, signing keys, and transactions.

Node — Trading platform

Bitcoin exchange

Users

Solo miner

Node — Block maker

Solo miners attempt to create blocks and mine them. The block maker and miner are the same person (compare with Mining Pools where the miners are a collective).

BITCOIN POINT OF SALE

- Bitcoin and other cryptocurrencies in the existing form or some other, will be the future of **online** payments

    - No cross border limits

    - As long as you have internet access, you can trade with it.

- however, will they work on real life scenarios? let's say to buy your coffee with Bitcoin?

    - **Requirements**:

        - A cafe to sell products with Bitcoin as a payment method

        - A user who is willing to spend Bitcoins for coffee

BITCOIN POINT OF SALE
IS IT STILL A THING? (2016)

- Cryptocurrencies are a fast paced technology

- Even though this experiment was started in late 2014 and data gathered in 2015, a few details would be considered as old and deprecated

- However, this is the second paper in the series of Usability of Bitcoin, which is a sub-field that has been underworked in cryptocurrencies (due to fast changing environment and and tech-savvy dominant community)

BITCOIN USABILITY

- On our first paper, we evaluated how usable Bitcoin is for end user.

A First Look at the Usability of Bitcoin Key Management

Shayan Eskandari[*], David Barrera[†], Elizabeth Stobert[‡], and Jeremy Clark[*]
[*]Concordia University, [†]ETH Zürich, [‡]Carleton University

http://www.internetsociety.org/sites/default/files/05_3_3.pdf

- **Conclusion**: A non-tech savvy user is most likely to do something wrong rather than get everything right.
  - somehow over simplified, but there's no perfect solution yet.

- **Result**: a framework to evaluate the usability of Bitcoin softwares

BITCOIN USABILITY

FOR THE COFFEE SELLER

- We used the same framework to evaluate existing Bitcoin Point of Sale approaches.

- These are our criteria for the framework:

- **Usability**:
  - User-friendly
  - Time-efficient
  - Fair Exchange Rate
  - Availability

- **Deployability**
  - Low Cost to Run
  - Enables Branching

- **Security**
  - No 3rd-Party Trust
  - Data Encryption
  - No Software Dependency

- **Privacy**
  - No Information Leakage
  - Maintains Payee's Privacy
  - Maintains Payer's Privacy
  - Confidential Payment list

BITCOIN USABILITY

FOR THE COFFEE SELLER

- Existing Bitcoin PoS approaches:

    - Static Bitcoin address stand

    - Hardware PoS Terminals

    - Online Merchant Services

    - Mycelium Gear

    - Aunja PoS

AUNJA* POS

DESIGN APPROACH

- We used a Scenario-Based Requirement Engineering method known as SCRAM**

- SCRAM has 4 steps:
  - Initial requirements capture and domain familiarization
  - Storyboarding and design visioning
  - Requirement exploration
  - Prototyping and requirement validation
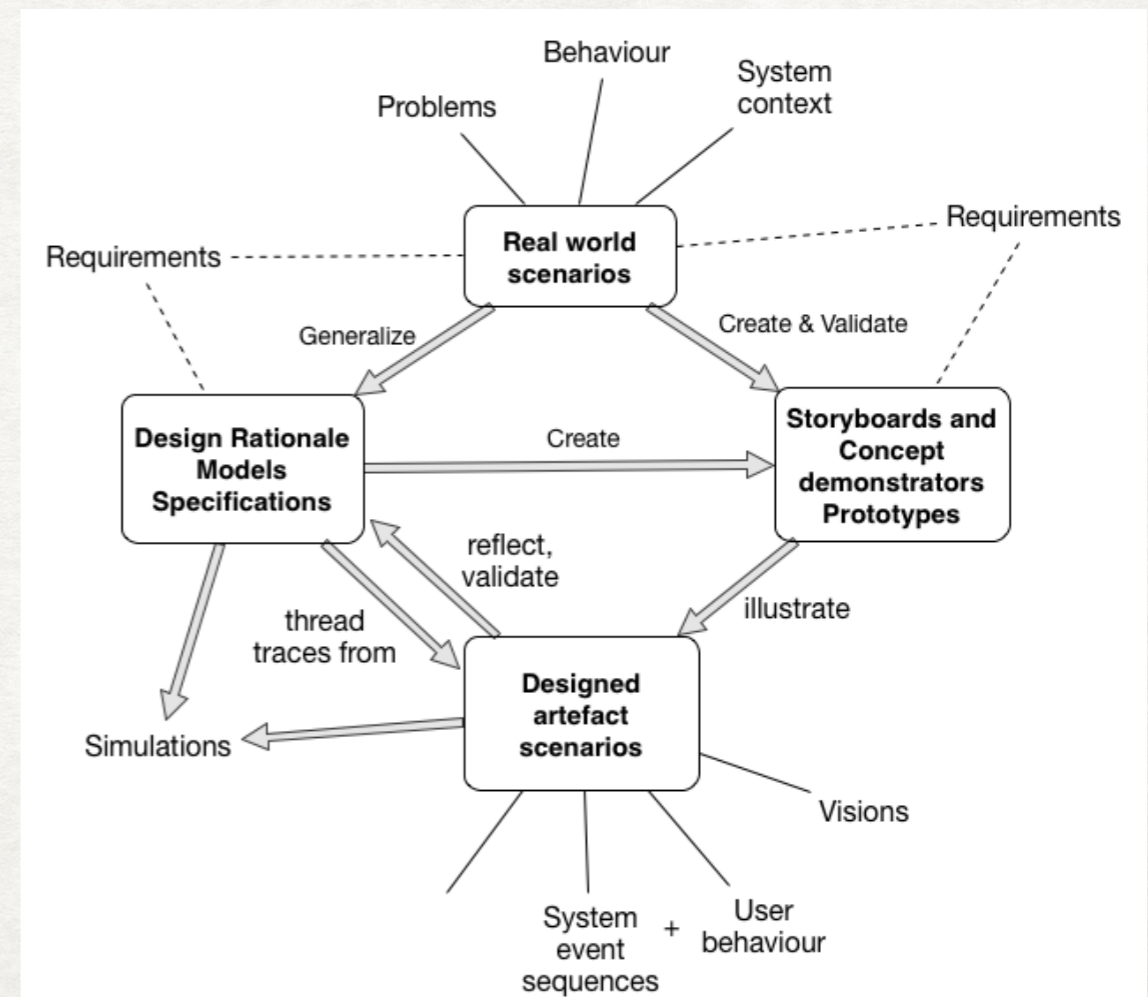
* Cafe Aunja - Montreal, QC, Canada
** Scenario-based Requirements Analysis Method

AUNJA POS

DESIGN APPROACH

- Initial requirements capture and domain familiarization
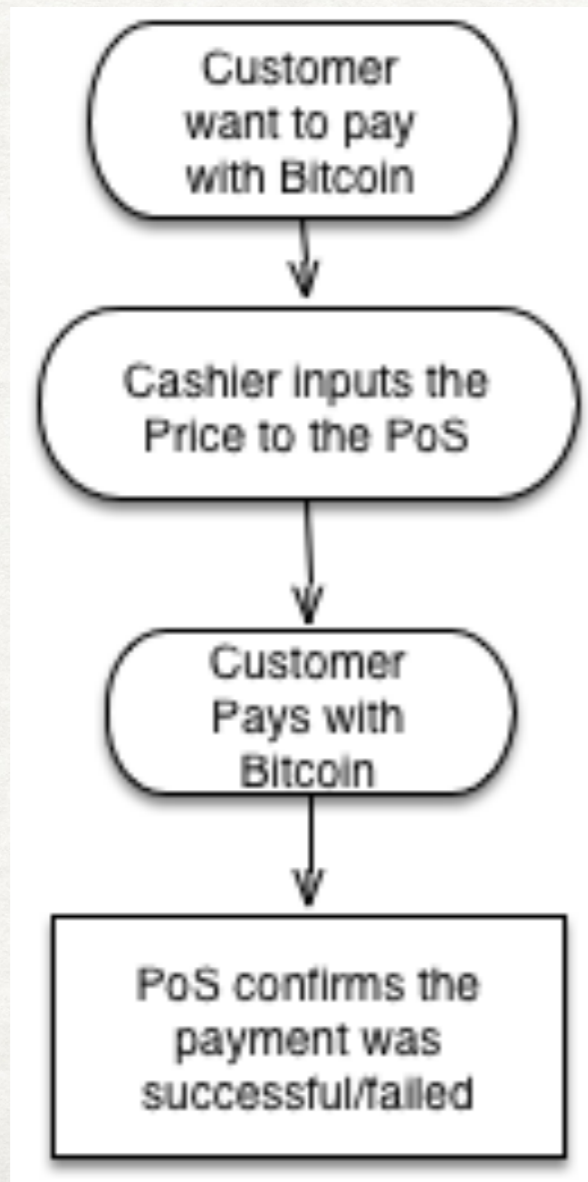
- Storyboarding and design visioning
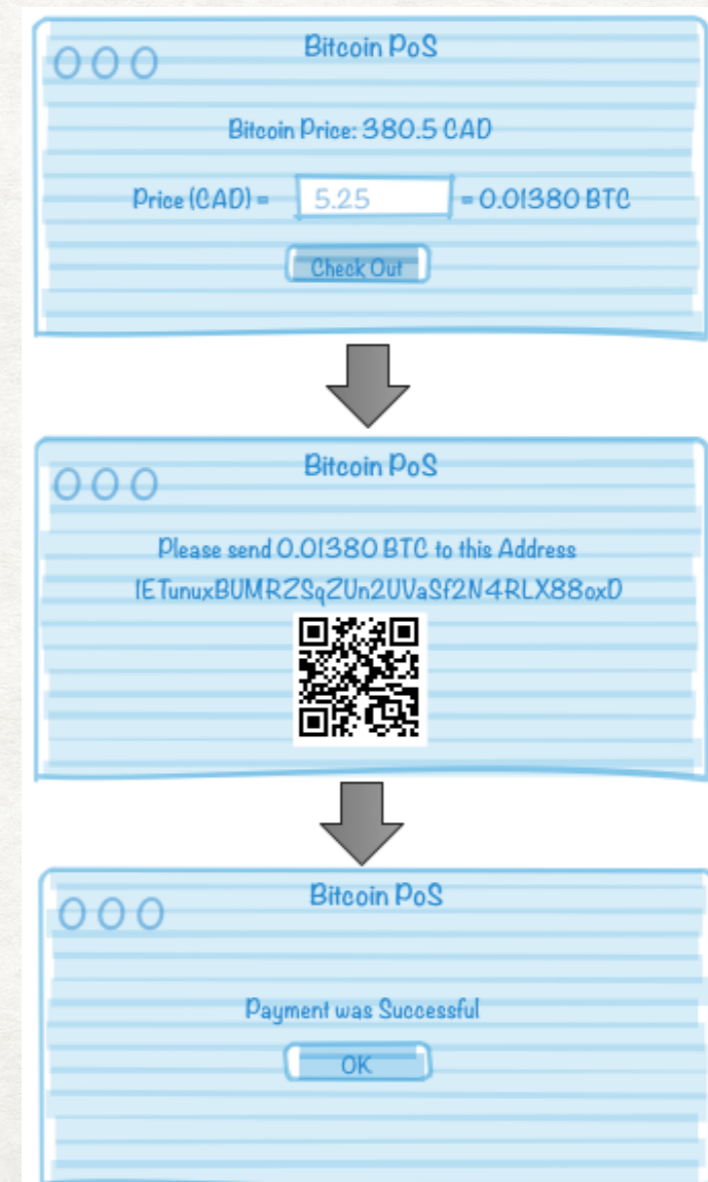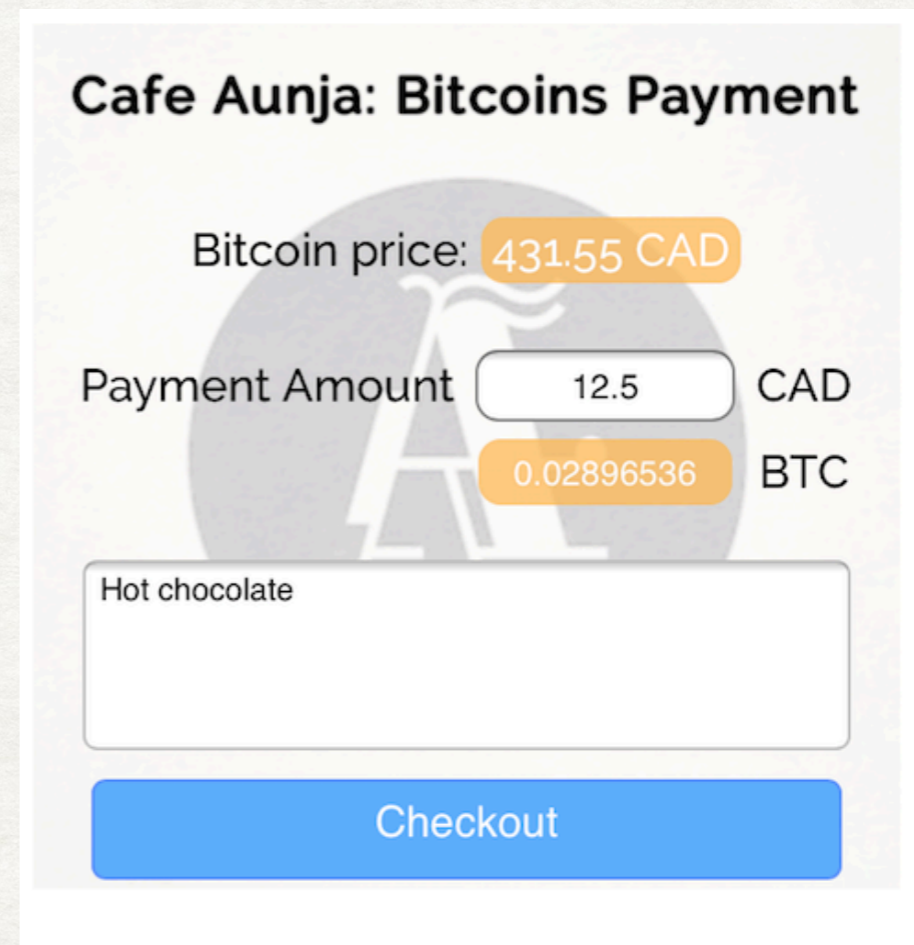
AUNJA POS

DESIGN APPROACH

- Requirement exploration

  - Going through the storyboards and scenarios to make sure we meet all the requirements

  - First round of feedbacks

- Prototyping and requirement validation

- First 4 are the existing methods, last one is the application we developed.

Category	User Friendly	Time-Efficient	Fair Exchange Rate	Availability	Low Cost to Run	Enables Branching	Maintains Payee's Privacy	Maintains Payer's Privacy	Confidential Payments list	No 3rd-Party Trust	Data Ecnryption	No Software Dependency
Displayed Address				●	●	○		○		●		●
Hardware Terminal	○	●	○	●			●	○	●		●	
Online Merchant Services	●	●	○	○	○	●	●	○	○		○	●
Mycelium Gear	○	●	○	○	○	●	●	○	○	○	○	○
Aunja PoS	●	●	●	●	○	○	●	○	●	●	●	○

(●) = Full score   (○) = Half score

- Still no perfect solution, however Aunja PoS approach is the closest.

- Released as Open souce project and Deployed in 2 other small businesses all over the world (https://github.com/shayanb/Bitcoin-PoS-PHP)

AUNJA POS

- Train employees using no technical jargons and concepts

- Answer customers questions, "What is Bitcoin?"
- Cashing Bitcoin earnings
  - Locked-Prices

Id	Date	Bitcoin Amount	Sale Dollar Amount	Note	Bitcoin Address
1	2015-04-18 14:12:33	4.68 CAD	3.5 CAD		1PKaQvzm3dXAHxYs7sb48ytahxxQzU8wKj
2	2015-05-07 13:46:15	29.33 CAD	23 CAD		17GTN1N2PKbyAfoSXtSkdfgHPeXwvVmY9x
3	2015-06-22 18:31:55	5.54 CAD	4.6 CAD		1FfYcmWiSnBmKdhEVRhsiVAC9GB6pZK3da
4	2015-06-22 18:32:17	6.75 CAD	5.6 CAD		12JKE6nGigN9VKuJQUvZSooekj5kPZ9dKT
Summary		46.30 CAD	36.7 CAD		

Technical Challenges:

- **Fast Verification of payments (Confirmation Time)**
 - Trade-off between Time and Risk of not getting paid
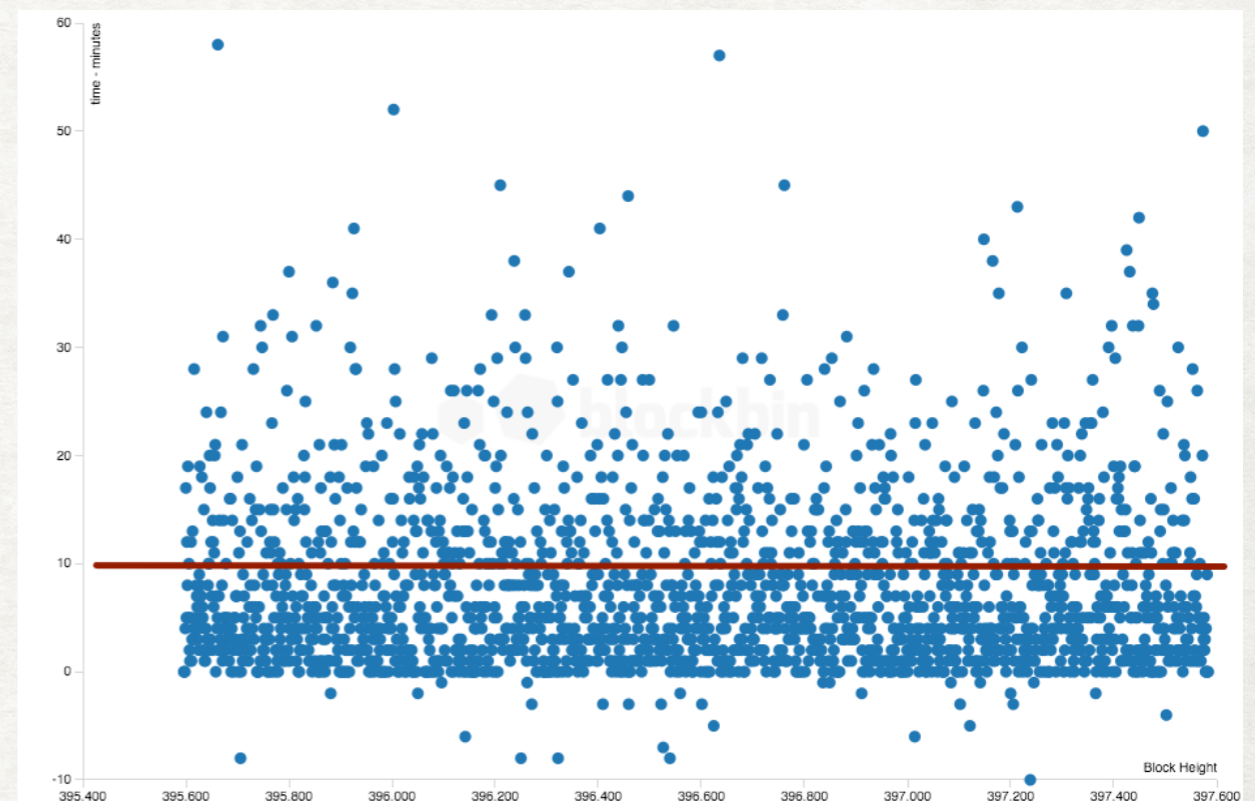
CONFIRMATION TIME
WHY BITCOIN POS MIGHT BE JUST A DREAM

- Bitcoin transactions should be mined and included in a block to be valid, otherwise there are ways to refuse to pay (double spend attack)

- Blocks are mined on average every 10 minutes

  - It might work when you buy a car but not a coffee

  - Also blocks are limited to 1MB and lately are mostly full (a.k.a Block-Size debate)
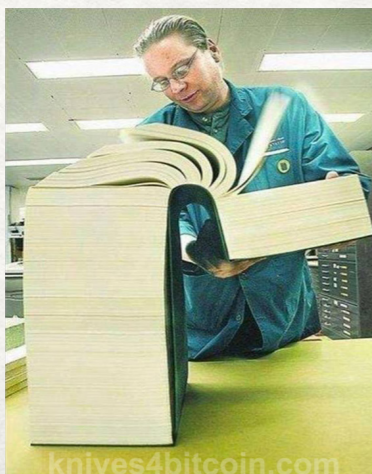
The Bitcoin block size debate is now available in this convenient paperback
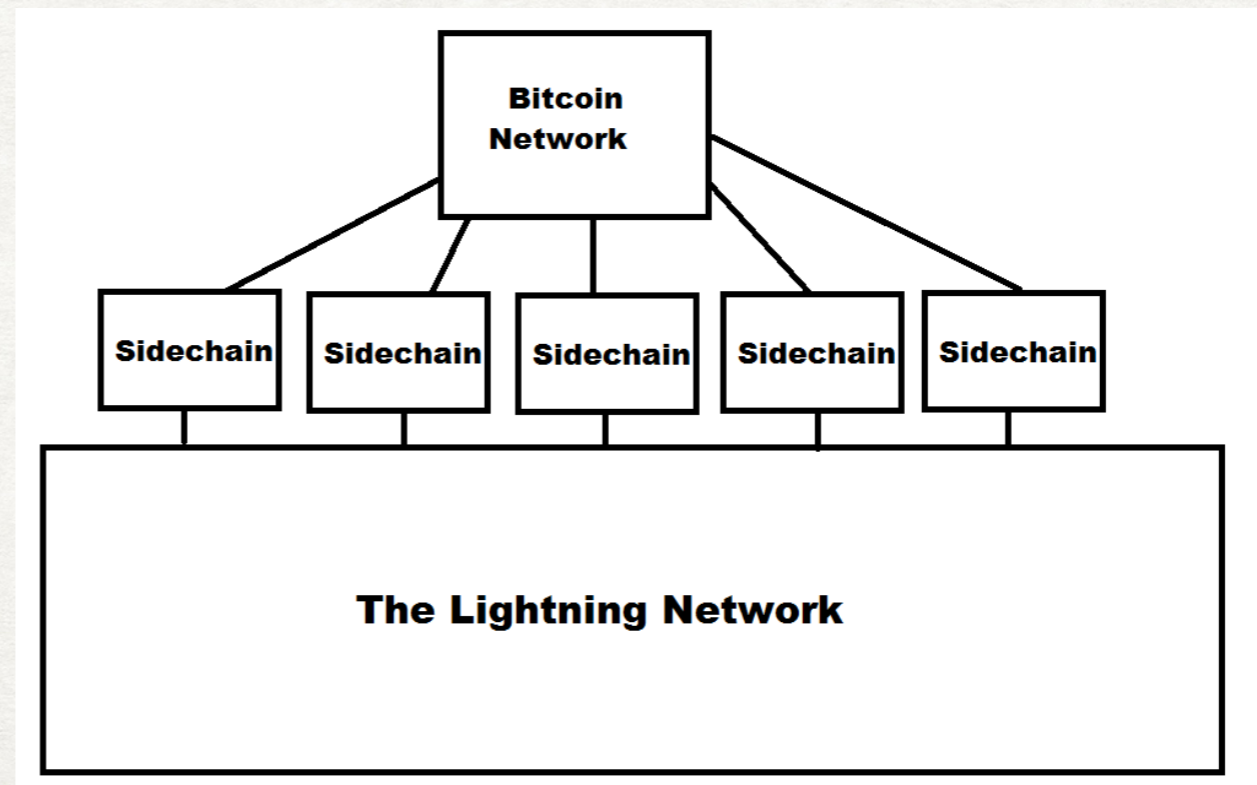
knives4bitcoin.com

CONFIRMATION TIME

WHY BITCOIN POS MIGHT BE JUST A DREAM

- This is still an open problem but there are proposed solutions

  - Alternative cryptocurrencies with shorter block time (e.g Ethereum block time is 15 seconds)

  - Bitgo Instant

  - Lightening Network

LET'S GET REAL FOR A MOMENT

- The idea of Bitcoin financial eco-system is utopian. Contactless payments are so convenient that no Bitcoin implementation can beat, although it can simply duplicate it via Bitcoin Debit cards.

- Also Bitcoin is a deflationary currency, meaning its price comparing to fiat currency would go up, so why spend it on coffee when you can tap and go with fiat currency?

- On the other hand, for international payments and money transfer, Bitcoin has the advantages of being purely digital.

  - Anyone with internet access can start using Bitcoin

  - No floor or ceiling limit on the amount you can transfer

    - Transferring 2 cents or 1 million dollar would cost you around 5 cents (Network mining fee to prevent continuos spamming and also mining incentives)

WHAT JUST HAPPENED?

SHOULD WE KEEP ON DREAMING?

- Bitcoin Point of Sale was a great way to add use cases for this currency, however it was misleading and didn't actually work the way it was supposed to.

- There are still multiple usability issues with Bitcoin softwares, mostly because of all the new concepts of money and financial systems it introduces

- There was no pragmatic way to know Bitcoin PoS would not become a real thing unless to deploy them in real world scenarios and see how people would react.

Cafe Aunja - October 2014

THANK YOU

" WRITING A DESCRIPTION FOR BITCOIN FOR GENERAL AUDIENCES IS BLOODY HARD. THERE'S NOTHING TO RELATE IT TO.

— *Satoshi Nakamoto*

"