



# **Predictive Markets: A Software Security Application**

Kushal Hebbar  
Jon Oakley

---

October 29, 2018

Clemson University

## Recap

---

# Goals

Recap

Current Status

Backup Slides

- Extend Augur's predictive market framework
- Metric for software security
- Feedback between software security and company performance
- *Emphasis on secure code*

# Architecture

Recap

Current Status

Backup Slides

- ✓ Ethereum and smart contracts
- ✓ Augur's prediction market framework
  - Marketplace frontend



ethereum



Augur (REP)



# Experimental Setup

Recap

Current Status

Backup Slides

- ~ ~~GENI testbed~~
  - Hardware Testbed (ECE Security Lab)
  - Augur Tool set for automatic market deployment
- ~ Augur APIs to link the market to the frontend
  - Naïve trading bots



## Current Status

---

# Current Timeline

Recap

**Current Status**

Backup Slides

Nov 5 Marketplace Frontend

Nov 5 Automatic Market Deployment

Nov 19 Trading Bots

# Lessons Learned

Recap

Current Status

Backup Slides

- Blockchain technology isn't perfect
- Integrating emerging technology isn't easy
- Open source documentation isn't always great
- Docker is a useful tool



Recap






Current Status

Backup Slides

WHY DO WHALES JUMP  
WHY ARE WITCHES GREEN  
WHY ARE THERE MIRRORS ABOVE BEDS  
WHY DO I SAY UH  
WHY IS SEA SALT BETTER  
WHY ARE THERE TREES IN THE MIDDLE OF FIELDS  
WHY IS THERE NOT A POKEMON MMO  
WHY IS THERE LAUGHING IN TV SHOWS  
WHY ARE THERE DOORS ON THE FREEWAY  
WHY ARE THERE SO MANY SUICIDE RUNNERS  
WHY AREN'T THERE ANY COUNTRIES IN ANTARCTICA  
WHY ARE THERE SORRY SOUNDS IN MINICRAFT  
WHY IS THERE KICKING IN MY STOMACH  
WHY ARE THERE TWO SLASHES AFTER HTTP  
WHY ARE THERE CELEBRITIES  
WHY DO SNAKES EXIST  
WHY DO OYSTERS HAVE PEARLS  
WHY ARE DUCKS CALLED DUCKS  
WHY DO THEY CALL IT THE CLAP  
WHY ARE KYLE AND CARTMAN FRIENDS  
WHY IS THERE AN ARROW ON PIANO'S HEAD  
WHY ARE TEXT MESSAGES BLUE  
WHY ARE THERE MUSTACHES ON CLOTHES  
WHY ARE THERE MUSTACHES ON CARS  
WHY ARE THERE MUSTACHES EVERYWHERE  
WHY ARE THERE SO MANY BIRDS IN OHIO  
WHY IS THERE SO MUCH RAIN IN OHIO  
WHY IS OHIO WEATHER SO WEIRD  
WHY ARE THERE MALE AND FEMALE BIKES  
WHY ARE THERE BIRDSPRINGS  
WHY DO DYING PEOPLE REACH UP  
WHY AREN'T THERE UNPLUGGED AIRPLANE  
WHY ARE OLD FURNACES IMPORTANT  
WHY ARE THERE SQUIRRELS  
WHY ARE THERE SQUIRRELS  
WHY IS PROGRAMMING SO HARD  
WHY IS THERE A 0 ON A RESERVOIR  
WHY DO PERSONS HAVE SCISSORS  
WHY DO RAINBOWS SOUND GOOD  
WHY DO TREES DIE  
WHY IS THERE NO SOUND ON GUN  
WHY AREN'T POKEMON REAL  
WHY AREN'T QUALITY SHIRT  
WHY DO DREAMS SEEM SO REAL  
WHY DO TESTICLES MOVE  
WHY ARE THERE PSYCHICS  
WHY ARE HATS SO EXPENSIVE  
WHY IS THERE CRYING IN TV SHAPES  
WHY DO YOUR BOOBS HURT  
WHY ARE THERE SLAVES IN THE BIBLE  
WHY DO TWINS HAVE DIFFERENT FINGERPRINTS  
WHY ARE AMERICANS AFRAID OF DRAGONS  
WHY IS HTTPS CROSSED OUT IN RED  
WHY IS THERE A LINE THROUGH HTTPS  
WHY IS THERE A RED LINE THROUGH HTTPS ON FACEBOOK  
WHY IS HTTPS IMPORTANT  
WHY AREN'T MY ARMS GROWING  
WHY ARE THERE MOSSES  
WHY DO I FEEL DIZZY  
WHY ARE THERE SO MANY CROUS IN ROCHESTER  
WHY IS PSYCHIC WEAK TO BUG  
WHY DO CHILDREN GET CANCER  
WHY IS POSEIDON ANGRY WITH ODYSSEUS  
WHY IS THERE ICE IN SPACE  
WHY ARE THERE EARTH TILTED  
WHY IS SPACE BLACK  
WHY IS OUTER SPACE SO COLD  
WHY ARE THERE PHANTOMS ON THE MOON  
WHY IS NASA SHUTTING DOWN  
WHY ARE THERE GHOSTS  
WHY ARE THERE TINY SPIDERS IN MY HOUSE  
WHY DO SPIDERS COME INSIDE  
WHY ARE THERE HUGE SPIDERS IN MY HOUSE  
WHY ARE THERE LOTS OF SPIDERS IN MY HOUSE  
WHY ARE THERE SPIDERS IN MY ROOM  
WHY ARE THERE SO MANY SPIDERS IN MY ROOM  
WHY DO SPIDER BITES ITCH  
WHY IS DYING SO SCARY  
WHY IS THERE NO GPS IN LAPTOPS  
WHY DO KNEES CLICK  
WHY AREN'T THERE E GRAPES  
WHY IS ISOLATION BAD  
WHY DO BOYS LIKE ME  
WHY DON'T BOYS LIKE ME  
WHY IS THERE ALLOWING A DRUM UPDATE  
WHY ARE THERE RED DOTS ON MY FACE  
WHY IS LYING GOOD  
WHY IS SEX SO IMPORTANT  
WHY IS MT VESUVIUS THERE  
WHY DO THEY SAY T MINUS  
WHY ARE THERE OBELISKS  
WHY ARE WRESTLERS ALWAYS WET  
WHY ARE OCEANS BECOMING MORE ACIDIC  
WHY IS ARWEN DYING  
WHY AREN'T MY QUAIL LAYING EGGS  
WHY AREN'T MY QUAIL EGGS HATCHING  
WHY AREN'T THERE ANY FOREIGN MILITARY BASES IN AMERICA  
WHY IS THERE AN OWL IN MY BACKYARD  
WHY IS THERE AN OWL OUTSIDE MY WINDOW  
WHY IS THERE AN OWL ON THE DOLLAR BILL  
WHY DO OWLS ATTACK PEOPLE  
WHY ARE AK 47s SO EXPENSIVE  
WHY ARE THERE HELICOPTERS CIRCLING MY HOUSE  
WHY ARE THERE GODS  
WHY ARE THERE TWO SPOOKS  
WHY ARE MY BOOBS ITCHY  
WHY ARE CIGARETTES LEGAL  
WHY ARE THERE DUCKS IN MY POOL  
WHY IS JESUS WHITE  
WHY IS THERE LIQUID IN MY EAR  
WHY DO Q TIPS FEEL GOOD  
WHY DO GOOD PEOPLE DIE  
WHY AREN'T THERE GUNS IN HARRY POTTER  
WHY ARE ULTRASOUNDS IMPORTANT  
WHY ARE ULTRASOUND FINANCES EXPENSIVE  
WHY IS STEALING WRONG

# QUESTIONS

FOUND IN GOOGLE AUTOCOMPLETE



## Backup Slides

---

# Development Environment

Recap

Current Status

Backup Slides

```
jon@ares:~$ ./augur.js
augur.js: 176x12
[2-26] gcnodes=240 gcsz=49.83kB gctime=620.038µs livenodes=400 liveness=242.23kB new block: 180, 1540780311 (Sun Oct 28 2018 22:31:51 GMT-0400 (EDT))
INFO [10-29] [02:32:15] block reached canonical chain number=199 hash=7a224f.b new block: 181, 1540780312 (Sun Oct 28 2018 22:31:52 GMT-0400 (EDT))
cf650 new block: 182, 1540780313 (Sun Oct 28 2018 22:31:53 GMT-0400 (EDT))
INFO [10-29] [02:32:15] mined potential block number=284 hash=901145.6 new block: 183, 1540780314 (Sun Oct 28 2018 22:31:54 GMT-0400 (EDT))
5f25c new block: 184, 1540780315 (Sun Oct 28 2018 22:31:55 GMT-0400 (EDT))
DEBUG [10-29] [02:32:15] Reinjecting stale transactions count=0 new block: 185, 1540780316 (Sun Oct 28 2018 22:31:56 GMT-0400 (EDT))
INFO [10-29] [02:32:15] Commit new mining work number=205 txs=0 uncles= new block: 186, 1540780317 (Sun Oct 28 2018 22:31:57 GMT-0400 (EDT))
0 elapsed=1.007ms new block: 187, 1540780318 (Sun Oct 28 2018 22:31:58 GMT-0400 (EDT))
INFO [10-29] [02:32:16] Successfully sealed new block number=205 hash=8f447a.62 new block: 188, 1540780319 (Sun Oct 28 2018 22:31:59 GMT-0400 (EDT))
2e0f new block: 189, 1540780320 (Sun Oct 28 2018 22:32:00 GMT-0400 (EDT))
DEBUG [10-29] [02:32:16] Trie cache stats after commit misses=0 unloads=0 new block: 190, 1540780321 (Sun Oct 28 2018 22:32:01 GMT-0400 (EDT))
nodes=0 size=8.808 tim new block: 191, 1540780322 (Sun Oct 28 2018 22:32:02 GMT-0400 (EDT))
e=2.27µs gcnodes=240 gcsz=49.83kB gctime=621.832µs livenodes=400 liveness=242.23kB new block: 192, 1540780323 (Sun Oct 28 2018 22:32:03 GMT-0400 (EDT))
INFO [10-29] [02:32:16] block reached canonical chain number=200 hash=28b0f4.6 new block: 193, 1540780324 (Sun Oct 28 2018 22:32:04 GMT-0400 (EDT))
27100 new block: 194, 1540780325 (Sun Oct 28 2018 22:32:05 GMT-0400 (EDT))
INFO [10-29] [02:32:16] mined potential block number=295 hash=8f447a.6 new block: 195, 1540780326 (Sun Oct 28 2018 22:32:06 GMT-0400 (EDT))
22e0f new block: 196, 1540780327 (Sun Oct 28 2018 22:32:07 GMT-0400 (EDT))
DEBUG [10-29] [02:32:16] Reinjecting stale transactions count=0 new block: 197, 1540780328 (Sun Oct 28 2018 22:32:08 GMT-0400 (EDT))
INFO [10-29] [02:32:16] Commit new mining work number=206 txs=0 uncles= new block: 198, 1540780329 (Sun Oct 28 2018 22:32:09 GMT-0400 (EDT))
0 elapsed=1.052ms new block: 199, 1540780330 (Sun Oct 28 2018 22:32:10 GMT-0400 (EDT))

[./src/reducers.js] 4.5 KiB [main] [built]
[./src/services/augur.js] 693 bytes [main] [built]
[./src/store.js] 3.76 KiB [main] [built]
[0] multi react react-dom redux redux-thunk moment react-datetime 88 bytes (assets/scripts/vendor) [built]
+ 2063 hidden modules
Child html-webpack-plugin for "index.html":
  Asset      Size  Chunks  Chunk Names
  index.html  1.4 KiB          0
  Entrypoint undefined = index.html
  [./node_modules/html-webpack-plugin/lib/loader.js!./src/index.ejs] 6.09 KiB (0) [built]
  [./node_modules/lodash/lodash.js] 527 KiB (0) [built]
  [./node_modules/webpack/buildin/global.js] (webpack)/buildin/global.js 489 bytes (0) [built]
  [./node_modules/webpack/buildin/module.js] (webpack)/buildin/module.js 497 bytes (0) [built]
[./index.html] Compiled successfully.
```

# Creating a Market

Recap

Current Status

Backup Slides

Create Market | Augur - Mozilla Firefox

localhost:8080/#/create-market

ETH: 158,456,324.923 / 5301  
USD: 11,098,599.653

DAI: 0.00000000 / 0  
BTC: 0.00000000 / 0

DAI PRICE (DAI) 20 (Market) 1.00  
Quintusid 0x913d...\_5430ab

CATEGORY / SOFTWARE TAGS / VERSION CONTROL

Git: 2.19.1

Outcome

VOLUME	FEE	MARKET OR GATOR FEE (0%)	REPORTING FEE (0.0000%)	EXPIRES
- ETH				-

MARKET QUESTION

Git: 2.19.1

The Augur platform does not work well for markets that are subjective or ambiguous. If you're not sure that the market's outcome will be known beyond a reasonable doubt by the expiration date, you should not create this market.

CATEGORY Software

SUGGESTED CATEGORIES

TAGS

Version Control

Tag 2

NEXT: OUTCOME

# Creating a Market

Recap

Current Status

Backup Slides

Create Market | Augur - Mozilla Firefox

localhost:8080/#/create-market

ETH: 158,456,324,923,5301  
USD: 11,099,599,653

Category: SOFTWARE  
Tags: VERSION CONTROL

Git: 2.19.1

70%

VOLUME	FEE	MARKET CREATOR FEE (2%) + REPORTING FEE (0.0008%)	EXPIRES
- ETH			-

MARKET TYPE

☒ Yes/No ☐ Multiple Choice ☐ Numerical Range

ADDITIONAL DETAILS

Optional: Include any additional information that traders should know about this market.

PREVIOUS: DEFINE

NEXT: RESOLUTION

# Creating a Market

Recap

Current Status

Backup Slides

The screenshot shows the 'Create Market' form in the Augur application, running in a Mozilla Firefox browser at localhost:8080. The form is divided into two main sections: a top section for market details and a bottom section for resolution and distribution options.

**Top Section:**

- CATEGORY:** SOFTWARE
- VERSION CONTROL:** Git: 2.19.1
- CURRENCY:** ETH
- MARKET CREATOR FEE (0%) + REPORTING FEE (0.0000%):** 100%
- EXPIRATION:** NOV 12, 2018 12:00 AM

**Bottom Section:**

- RESOLUTION SOURCE:** ☒ General knowledge, ☐ Outcome will be detailed on a public website
- DISTRIBUTION MECHANISM:** ☒ Myself, ☐ Someone Else
- EXPIRATION DATE:** Nov 12, 2018
- EXPIRATION TIME (UTC-6):** 12:00 AM
- Buttons:** PREVIOUS OUTCOME, NEXT LIQUIDITY



# Creating a Market

Recap

Current Status

Backup Slides

Create Market | Augur - Mozilla Firefox

localhost:8080/#/create-market

ETH: 158,456,324,923.5301  
USD: 11,098,999.6553

Git: 2.19.1

VOLUME	FEE	CURREN
- ETH	MARKET CREATOR FEE (2%) + REPORTING FEE (1.0000%)	NOV 12, 2018 12:00 AM

### CONFIRM MARKET

MARKET CREATION		MARKET LIQUIDITY	
VALUITY BOND	0.0100 ETH	ETH	0.0000 ETH
NO SHOW BOND	0.3497 REP	EST SAS	0.0000 ETH
EST SAS	0.0513 ETH		

RESOLUTION SOURCE  
General Incentivized gas

DESIGNATED REPORTER  
Myself

ADDITIONAL DETAILS  
None

PREVIOUS LIQUIDITY

SUBMIT

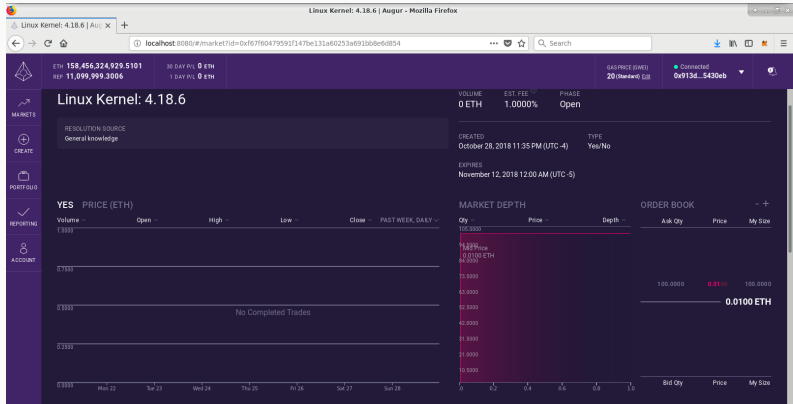


# Trading

Recap

Current Status

Backup Slides



# Trading

Recap

Current Status

Backup Slides

Linux Kernel: 4.18.6 | Augur - Mozilla Firefox

ETH 158,456,324,929.5101  
REP 11,099,999.3006

30 DAY P/L 0 ETH  
1 DAY P/L 0 ETH

BAS PRICE (BWD)  
20 (Standard) Est

Connected  
0x013d...5430eb

0.0001 0.0002 0.0003 0.0004 0.0005 0.0006 0.0007 0.0008 0.0009 0.0010

0.0 0.5 1.0 Bid Qty Price My Size

MARKETS

CREATE

PORTFOLIO

REPORTING

ACCOUNT

OUTCOMES

OUTCOME	BID QTY	BEST BID	BEST ASK	ASK QTY	LAST
• Yes 50.00%	—	—	0.0100	100.0000	—

MY POSITIONS

OPEN ORDERS	QUANTITY	AVERAGE PRICE	ESCROWED ETH	ESCROWED SHARES	ACTION
Yes	-100.0000	0.0100	99.0000	0	Cancel

BUY SELL

QUANTITY 0.00000001 Shares

LIMIT PRICE 0.0001 ETH

☐ FILL ORDERS ONLY

EST. COST 0 ETH  
0 Shares

REVIEW

# Positions

Recap

Current Status

Backup Slides

