Lab 00:
Blockchain for Developers

Nick Zoghb

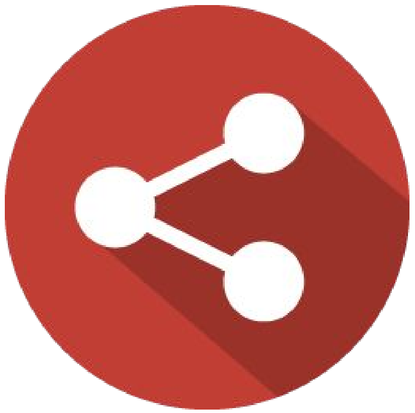
LAB OUTLINE

1. WELCOME
2. CLASS OUTLINE
3. WHY WORK IN THE SPACE
4. EXERCISE: ENVIRONMENT SETUP

1 WELCOME

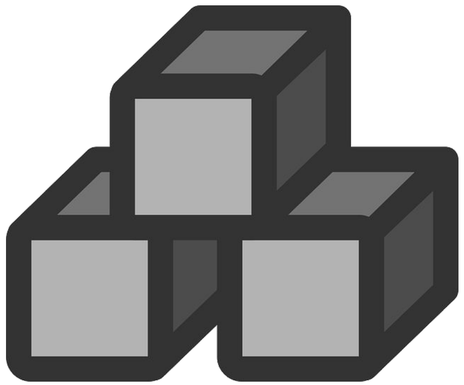
THE COURSE

WELCOME TO BLOCKCHAIN FOR DEVELOPERS



Protocol Development

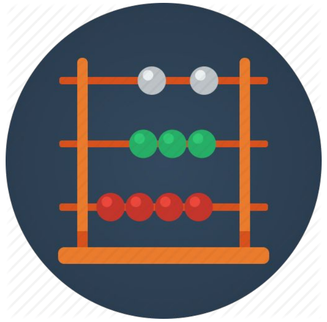
Cryptoeconomics



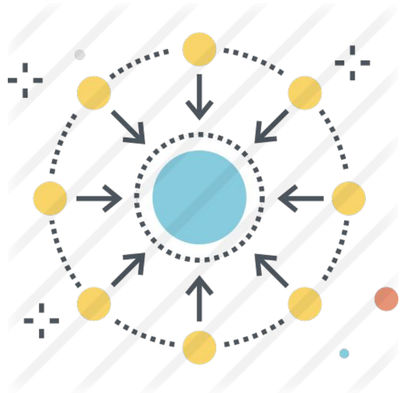
Blockchain Fundamentals

Đapp Development

Security

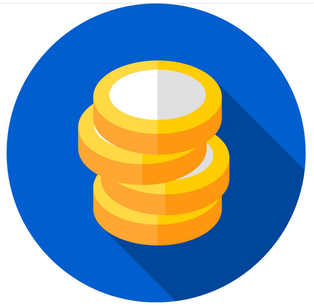


Cryptographic Primitives



Consensus

Async Testing



Building Token Sales (ICO)

AKASH KHOSLA

WHO IS HE?

- Head of Internal
  - Co-founder of Blockchain at Berkeley
  - Leads recruitment and helps push manage internal matters
  - Previously Head of Design
- Software Engineering Intern at Earn.com (previously 21.co)
  - Went to IC3 this summer where I worked with Phil Daian on smart contract security (security researcher at Cornell)
- 3rd Year, Electrical Engineering and Computer Science
- Previously worked in John Canny's lab on BIDMach, a high performance machine learning library

NICK ZOGHB

WHO IS HE?

- Co-Head of Education at Blockchain at Berkeley
  - Working on Vyper documentation
  - Help facilitate this course
  - TA for CS 294-144
- Data Engineering Intern at Cisco, Tesloop
  - Went to IC3 last summer; worked with Dan Robinson on Chain's Ivy compiler
- 4th Year, Computer Science w/BioE Minor
- Worked in Jack Gallant's computational neurobiology lab

THE TEAM

WHO ARE THEY?

LUKE STRGAR
TEACHING ASSISTANT

NICHOLAS TRUONG
TEACHING ASSISTANT

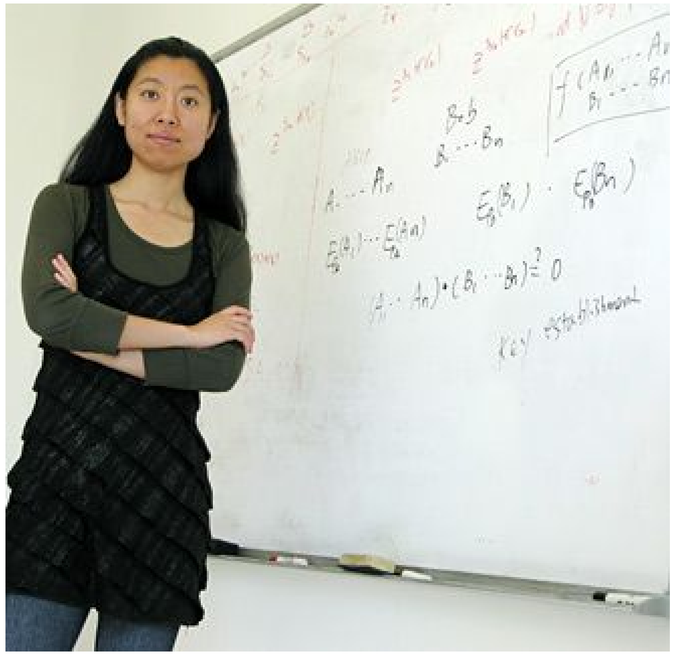
NATALIYA URAKHCHINA
TEACHING ASSISTANT

ADDITIONAL INFORMATION

THINGS TO LOOK OUT FOR

Please be sure to note the following

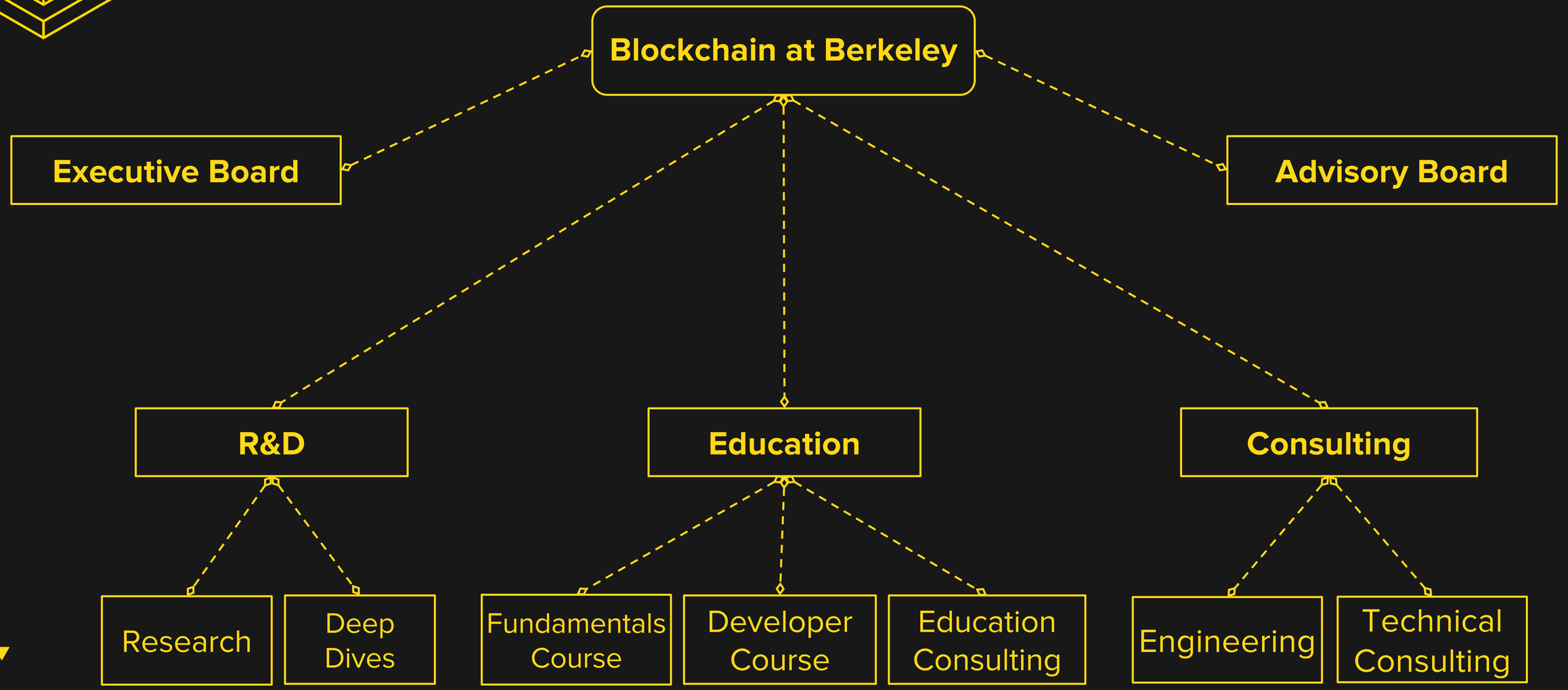
- Course Control Number (CCN): 42562
- Faculty sponsor: Dawn Song
- Piazza, sign-up URL: http://piazza.com/berkeley/spring2018/cs19878
- Email (for urgent matters): dev-decal@blockchain.berkeley.edu
- Official website: TBD
  - Lab assignments
  - Readings



BITCOIN
Association of Berkeley

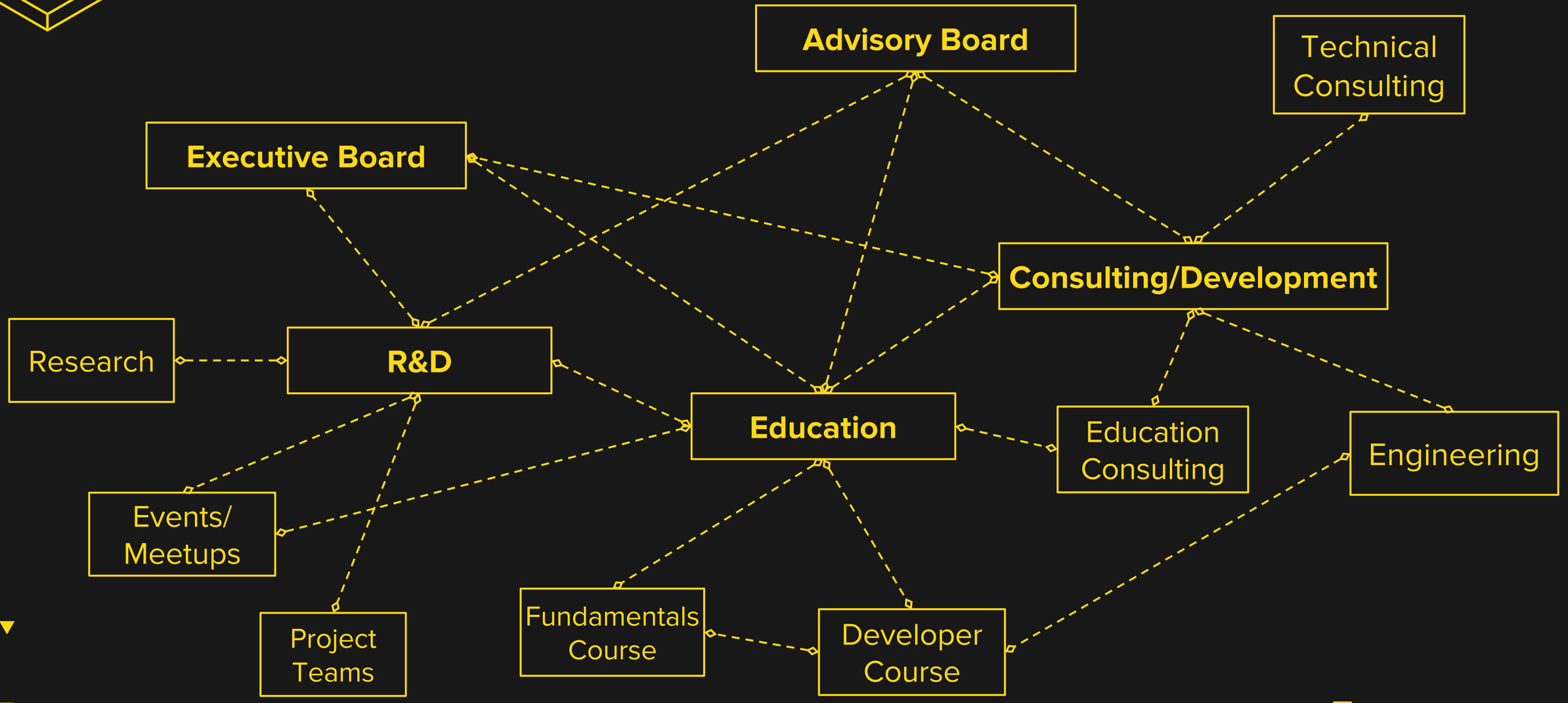
BLOCKCHAIN
AT BERKELEY

WHO ARE WE



BLOCKCHAIN AT BERKELEY

WHO ARE WE



BLOCKCHAIN AT BERKELEY

2 CLASS OUTLINE

EXPECTATIONS

ADMINISTRIVIA

What to expect from us:

- Review of Blockchain Fundamentals concepts
- Technical, in-depth talks that can go as far down as the protocol code
- Rewarding programming assignments and group projects
- A mildly frustrating, but extremely unique experience that you can’t find elsewhere
- Help on Piazza and during Labs
- A collated compendium of knowledge that is otherwise scattered across the interwebs

EXPECTATIONS

ADMINISTRIVIA

What we expect from you:

- Dedication - treat this course as a 2-unit class
- Attention and readiness to learn (attendance + participation = 30% grade)
  - You have two freebies, after that, unexcused absences take 10% of this grade
    - More than 3 absences result in auto-fail
- Come to office hours (after class), talk on Piazza
- CS61A minimum, CS61B recommended, fundamental CS concepts needed

WEEKLY SCHEDULE

LAB + LECTURE

LAB 00

Thursday, February 1st

Blockchain for Developers

LECTURE 01

Friday, February 2nd

Introduction to Blockchain

LAB 01

Thursday, February 8th

Solidity in Depth

LECTURE 02

Friday, February 9th

Ethereum's Smart Contracts

AUTHOR: NICK ZOGHB

BLOCKCHAIN
AT BERKELEY

LAB 02

Thursday, February 15th

Baby's First ICO

LECTURE 03

Friday, February 16th

Asynchronous Testing

LAB 03

Thursday, February 22nd

Smart Contract Architecture

LECTURE 04

Friday, February 23rd

Smart Contract Security

LAB 04

Thursday, March 1st

Attack the Auction

LECTURE 05

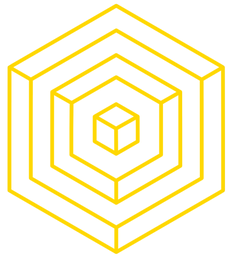
Friday, March 2nd

Web3 and Front End Integration

A NOTE ON ELECTRONICS

PARTICIPATE IN LAB

- Please come to lab with charged devices
- There are not enough outlets in HP Auditorium
- There will be live coding, you may want to follow along!
- If you finish lab, there is no homework



3 WHY DEVELOP?

WHY EVEN BOTHER?

WHY IS BLOCKCHAIN DEVELOPMENT A THING?

- High demand, low supply of developers
  - Blockchain at Berkeley fills a critical market niche
- It’s early, much akin to the web revolution of the 90’s
  - Even some parallels to the dot-com bubble
  - Is this a cryptocurrency bubble?
- To the majority of people blockchain is just a buzzword
- Even if blockchain isn’t the future, working in the space yields valuable insight
  - Application to distributed systems, cryptography, security, and more!

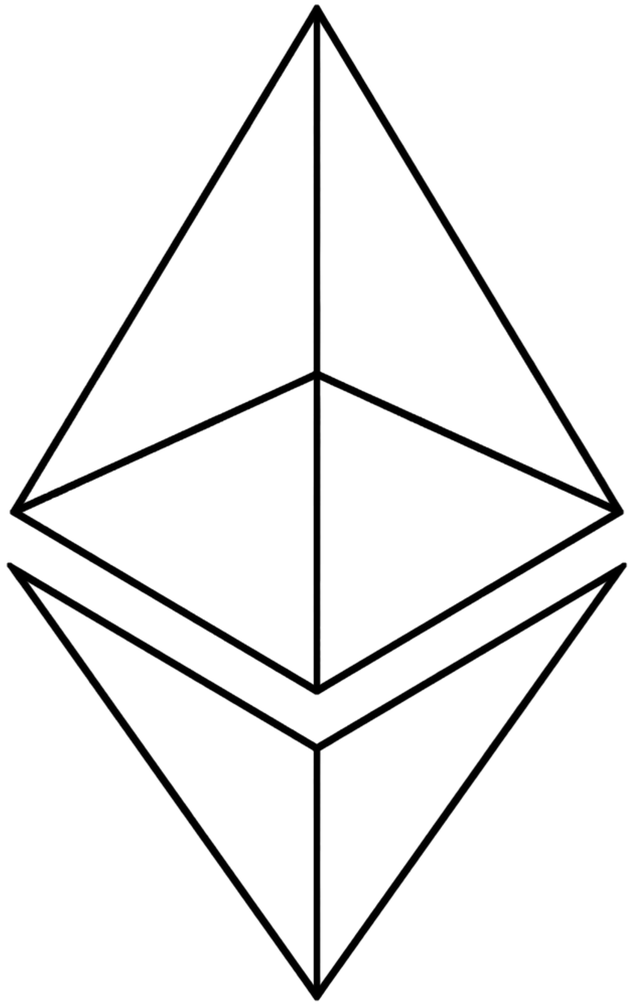
MORE REASONS

WHY IS BLOCKCHAIN DEVELOPMENT A THING?

- Very open community
  - Accessible to anyone, most of the code is open source
- Niche but also not too competitive
- Not too hard to get ahead and easily get a job or internship
  - Plenty of Blockchain at Berkeley members ended up with internships at ConsenSys, Lightning Network, earn.com (21.co), BlockApps, SAP, and other companies involved in blockchain initiatives
  - B@B also does education consulting

4 EXERCISE

*Optional



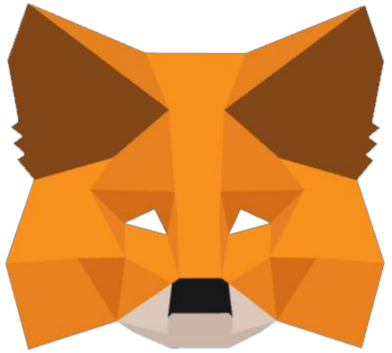
HOMEBREW

Essential macOS package manager

GETH

The Go-Ethereum client

```
brew tap ethereum/ethereum
brew install ethereum
```



METAMASK*

Browser extension; acts as interface to Đapps

SOLC*

Solidity compiler

```
brew install solidity
```

DIVE INTO GETH

TRY IT OUT!

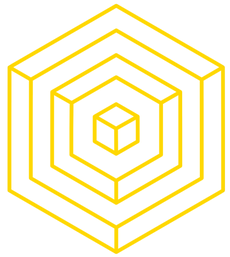
- Use `geth` to sync up with the *Rinkeby* testnet (should take some time), use `geth help` if confused

```
$ geth --rinkeby --syncmode "fast"
$ geth --datadir=$HOME/.rinkeby attach ipc:$HOME/Library/Ethereum/rinkeby/geth.ipc console
```

- Create an account and remember the password! There is no “I forgot my password” option
  - See this xkcd comic

```
> personal.newAccount("password")
> eth.coinbase
> eth.getBalance(eth.coinbase)
```

- Post your address (the output of `eth.coinbase`) to a public social media outlet, see this example.
  - Post the link here



DIVE INTO GETH

SOME NOTES

- Ok but where does “chaindata” go?

```
$ geth --rinkeby --syncmode "fast"
```

  - On macOS: *~/Library/Ethereum*

- *Rinkeby* uses *Proof of Authority*!

```
INFO [02-01|12:58:42] Imported new block headers      count=192 elapsed=68.855ms number=4416 hash=1e5c33…393dd5 ignored=0
INFO [02-01|12:58:45] Imported new block headers      count=192 elapsed=65.695ms number=4608 hash=538b29…780c13 ignored=0
INFO [02-01|12:58:45] Imported new block headers      count=192 elapsed=65.885ms number=4800 hash=50820a…4b337d ignored=0
INFO [02-01|12:58:45] Imported new block headers      count=192 elapsed=70.070ms number=4992 hash=ad12ee…6f5b42 ignored=0
INFO [02-01|12:58:45] Imported new block headers      count=192 elapsed=63.923ms number=5184 hash=c928d6…764b9f ignored=0
INFO [02-01|12:58:46] Imported new block headers      count=192 elapsed=67.020ms number=5376 hash=6d6b63…16e7a2 ignored=0
INFO [02-01|12:58:46] Imported new block headers      count=192 elapsed=80.542ms number=5568 hash=93f0f8…fdebf3 ignored=0
INFO [02-01|12:58:46] Imported new block headers      count=192 elapsed=75.313ms number=5760 hash=1ff4ac…0a423a ignored=0
INFO [02-01|12:58:46] Imported new block headers      count=192 elapsed=82.164ms number=5952 hash=7875aa…590407 ignored=0
INFO [02-01|12:58:47] Imported new block headers      count=192 elapsed=80.146ms number=6144 hash=263d8e…5672a9 ignored=0
INFO [02-01|12:58:47] Imported new block headers      count=192 elapsed=69.836ms number=6336 hash=49dcf2…ae2dc0 ignored=0
INFO [02-01|12:58:47] Imported new block headers      count=192 elapsed=68.809ms number=6528 hash=eb8557…5cc3d9 ignored=0
INFO [02-01|12:58:49] Imported new block headers      count=192 elapsed=63.426ms number=6720 hash=288a07…da6bbb ignored=0
INFO [02-01|12:58:49] Imported new block headers      count=192 elapsed=64.134ms number=6912 hash=32c9f0…9b2a1f ignored=0
INFO [02-01|12:58:50] Imported new block headers      count=192 elapsed=69.062ms number=7104 hash=40562e…b55f7a ignored=0
INFO [02-01|12:58:50] Imported new block headers      count=192 elapsed=65.466ms number=7296 hash=88456b…649948 ignored=0
INFO [02-01|12:58:51] Imported new block headers      count=192 elapsed=66.427ms number=7488 hash=add5a8…599711 ignored=0
INFO [02-01|12:58:53] Imported new block headers      count=192 elapsed=65.152ms number=7680 hash=e68fae…c866dc ignored=0
INFO [02-01|12:58:55] Imported new block headers      count=192 elapsed=66.265ms number=7872 hash=8eaf10…c27981 ignored=0
INFO [02-01|12:58:55] Imported new block headers      count=192 elapsed=68.923ms number=8064 hash=c8dc8b…64e353 ignored=0
INFO [02-01|12:58:55] Imported new block headers      count=192 elapsed=71.002ms number=8256 hash=d6de11…235678 ignored=0
INFO [02-01|12:58:56] Imported new block headers      count=192 elapsed=65.205ms number=8448 hash=9c501c…54faa1 ignored=0
INFO [02-01|12:58:56] Imported new block headers      count=192 elapsed=63.575ms number=8640 hash=19e90f…9aaf7f ignored=0
INFO [02-01|12:58:57] Imported new block headers      count=192 elapsed=75.969ms number=8832 hash=7d3e5b…d27c91 ignored=0
INFO [02-01|12:58:59] Imported new block headers      count=192 elapsed=68.462ms number=9024 hash=6705c6…078ee7 ignored=0
INFO [02-01|12:58:59] Imported new block headers      count=192 elapsed=77.279ms number=9216 hash=b36021…f89062 ignored=0
INFO [02-01|12:59:01] Imported new block headers      count=192 elapsed=65.118ms number=9408 hash=85d92c…070136 ignored=0
INFO [02-01|12:59:02] Imported new block headers      count=192 elapsed=105.644ms number=9600 hash=e5d5d5…3a6f1e ignored=0
INFO [02-01|12:59:04] Imported new block headers      count=192 elapsed=72.040ms  number=9792 hash=bac424…3fb3aa ignored=0
INFO [02-01|12:59:07] Imported new block headers      count=192 elapsed=68.521ms  number=9984 hash=adf097…969c56 ignored=0
INFO [02-01|12:59:10] Imported new block headers      count=192 elapsed=82.696ms  number=10176 hash=ca7432…e49656 ignored=0
INFO [02-01|12:59:12] Imported new block headers      count=192 elapsed=73.351ms  number=10368 hash=70e8a0…679d77 ignored=0
INFO [02-01|12:59:17] Imported new block headers      count=192 elapsed=69.178ms  number=10560 hash=fe1de1…342226 ignored=0
INFO [02-01|12:59:20] Imported new block headers      count=192 elapsed=69.667ms  number=10752 hash=7360ad…618226 ignored=0
INFO [02-01|12:59:21] Imported new block headers      count=192 elapsed=67.235ms  number=10944 hash=c69857…e0f549 ignored=0
INFO [02-01|12:59:23] Imported new block headers      count=192 elapsed=73.679ms  number=11136 hash=0b8fed…73a25a ignored=0
INFO [02-01|12:59:25] Imported new block headers      count=192 elapsed=72.865ms  number=11328 hash=d3cea3…078eab ignored=0
INFO [02-01|12:59:28] Imported new block headers      count=192 elapsed=67.282ms  number=11520 hash=2d524c…110f74 ignored=0
INFO [02-01|12:59:28] Imported new block headers      count=192 elapsed=65.903ms  number=11712 hash=44e2d5…0a8611 ignored=0
INFO [02-01|12:59:29] Imported new block headers      count=192 elapsed=73.039ms  number=11904 hash=65ef79…270798 ignored=0
INFO [02-01|12:59:29] Imported new block headers      count=192 elapsed=70.707ms  number=12096 hash=b44066…ddc72b ignored=0
INFO [02-01|12:59:29] Imported new block headers      count=192 elapsed=88.361ms  number=12288 hash=505675…2b29ca ignored=0
INFO [02-01|12:59:30] Imported new block headers      count=192 elapsed=71.469ms  number=12480 hash=b9c6f9…e3b84d ignored=0
INFO [02-01|12:59:30] Imported new block headers      count=192 elapsed=66.489ms  number=12672 hash=81a15e…f7933e ignored=0
INFO [02-01|12:59:30] Imported new block headers      count=192 elapsed=66.850ms  number=12864 hash=003920…efbd44 ignored=0
INFO [02-01|12:59:32] Imported new block headers      count=192 elapsed=65.947ms  number=13056 hash=b9d9d9…dc79c4 ignored=0
INFO [02-01|12:59:35] Imported new block headers      count=192 elapsed=66.532ms  number=13248 hash=ce671c…4e74de ignored=0
```

```
WARN [02-01|12:58:04] Light client mode is an experimental feature
```

DIVE INTO GETH

TRY IT OUT!

- Check your balance again!

```
> eth.getBalance(eth.coinbase)
300000000000000000
```

- While you're at it, check out these cool data visualizations of network stats :

NODE.JS

A useful JavaScript library

NPM

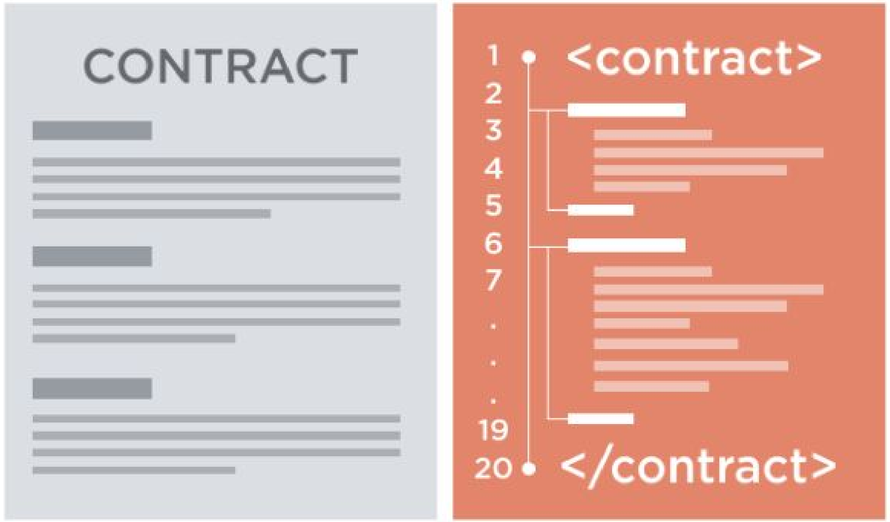
JavaScript package manager

TRUFFLE

Incredibly useful development environment and testing framework

GANACHE/TESTRPC

Simulation of full client behavior



THINGS TO THINK ABOUT

UH-OH, TIME TO WORK

Try to come up with answers to the following questions:

- What is the difference between “light”, “fast”, and “full” geth syncmodes?
- Why use a testnet over mainnet?
- What is Proof of Authority?

QUESTIONS?

SEE YOU NEXT TIME

Introduction to Blockchain

Consensus

Public-Key Cryptography

Digital Signatures

Hash Functions

Transactions

Bitcoin

Mining

BLOCKCHAIN AT BERKELEY