Crypto for the People (Part 2)

Seny Kamara

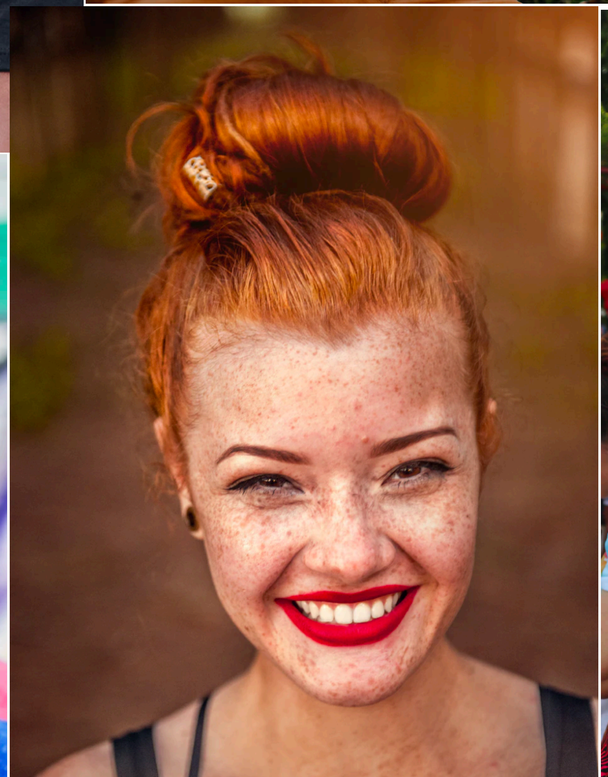
BROWN

ENCRYPTED SYSTEMS LAB


DAMN.

Who Benefits from Cryptography?



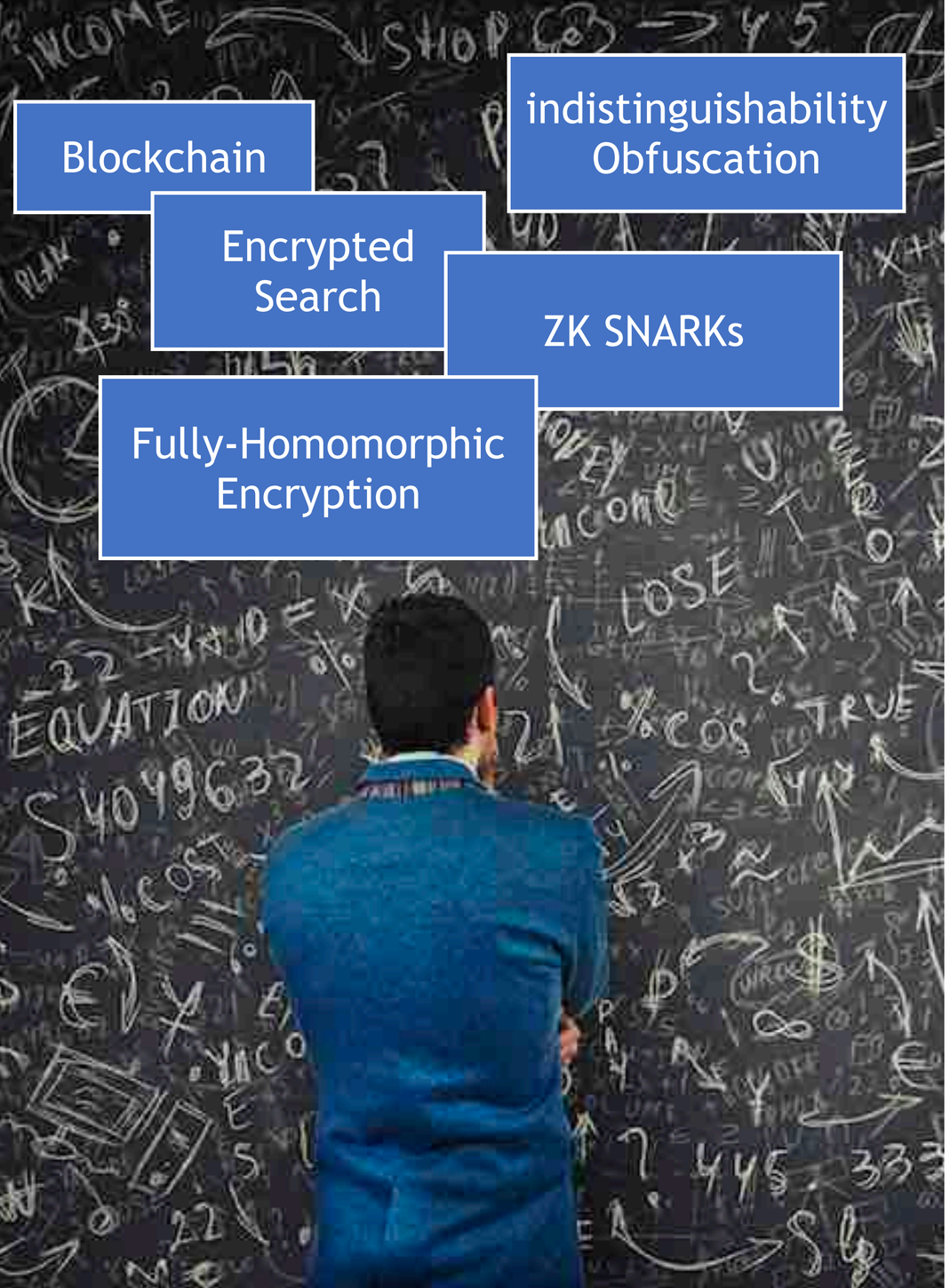



CRYPTO ’20 Talk

Not Crypto for the People

- My new blockchain will
  - serve rural communities in Africa
  - “solve long-standing developmental issues & unlock much-needed economic growth”
- Doing it wrong
  - using marginalized groups to motivate your existing research or product
- Doing it right
  - new research/tech to address problems experienced by marginalized groups
  - *in consultation with experts*

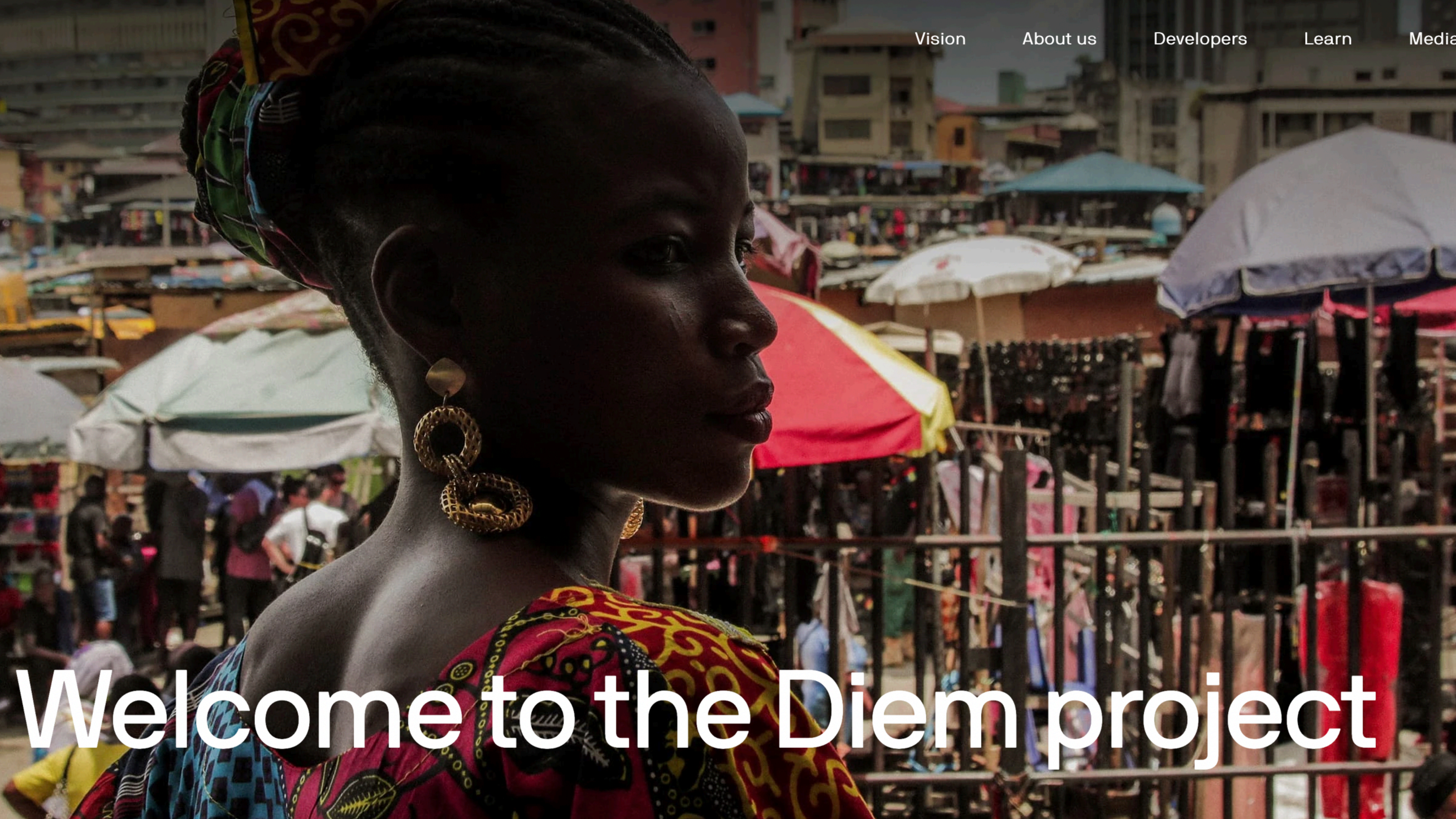

DO YOU
EVEN
CRYPTO,
BRO?



- Bob likes fancy cryptography
- Bob notices people talking about
  - police violence
  - sexual harassment & assault
  - bias & discrimination in ML
  - misinformation in social networks
- Bob thinks
  - “I’ll use crypto to solve police violence!”

Why is this a Problem?

- Bob is not really interested in the social problem
- Bob is interested in…
  - …*the crypto problem he claims is motivated by the social problem*
- While the crypto problem is “fun” it does not address the real problem
- Bob has a hammer and is looking for a “social nail”



Welcome to the Diem project

Marginalized Groups as Branding

- Wanting to help address social problems is great

- But often people are just using
  - marginalized communities & social problems as branding
  - “Crypto-currencies for developing countries”
  - “Fintech for the unbanked”
  - “AI teachers and chatbots for poor and underserved areas”

What Should Bob Do?

- If Bob genuinely cares about a social problem

- He should work with experts
  - experts in social sciences & humanities
  - experts with lived experience

- Lived experience is crucial because
  - the details really matter
  - the psychological state really matters
  - the broader context really matters

Collaboration

- Experts
  - know which assumptions make sense and which do not
  - know of crucial practical constraints
  - understand the human/psychological dimensions of the problem
  - know which risks are tolerable and which are not
  - can see potential harms that you cannot see

- Bob should design what the experts believe is useful…
  - …even if the crypto/tech is “boring”


U.S. GUN
CONTROL

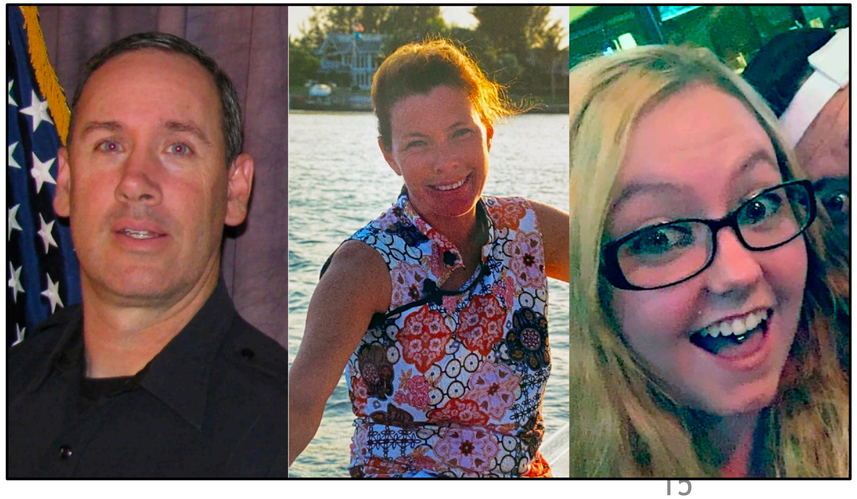
Gun Violence

- *36,000* Americans killed & *100,000* injured by guns every year
- *600* Women shot & killed by intimate partner every year
- *4.5 million* Women threatened with a gun every year
- Black people *10x* more likely to be killed with a gun than Whites
- Black men account for *52%* of gun deaths

Gun Violence: Mass Shootings

- 1966-2012: *30%* of mass shootings in the world occurred in US

- Movie theaters, Night Clubs, Concerts, Universities, High Schools, Elementary Schools, Spas and Grocery Stores



Gun Control Laws in the U.S.

- Omnibus Crime Control and Safe Streets Act of 1968
  - prohibits interstate sale of firearms and raised minimum age to 21

- Gun Control Act of 1968
  - Requires sellers to be licensed

- Brady Act of 1993
  - Requires sellers to do background checks

- Firearm Owner Protection Act (FOPA) of 1986
  - Federal government and states cannot require gun registration

Encrypted Gun Registry

- Early 2019: Sen. Wyden' s (D-OR) staff reaches out

- Draft bill for voluntary & decentralized national gun registry
  - local databases encrypted & managed by local officials
  - but can be queried by law enforcement
  - Federal & State Government cannot see any of the data
  - local officials can "pull" their data at any time?

Encrypted Gun Registry

- Built & evaluated a prototype

  - 400M records with largest county holding 50M
  - 300ms to identify the county a gun is in
  - (at most) 1 minute to query an encrypted local database
  - 45m to add 10,000 records
  - less than $100,000 a year

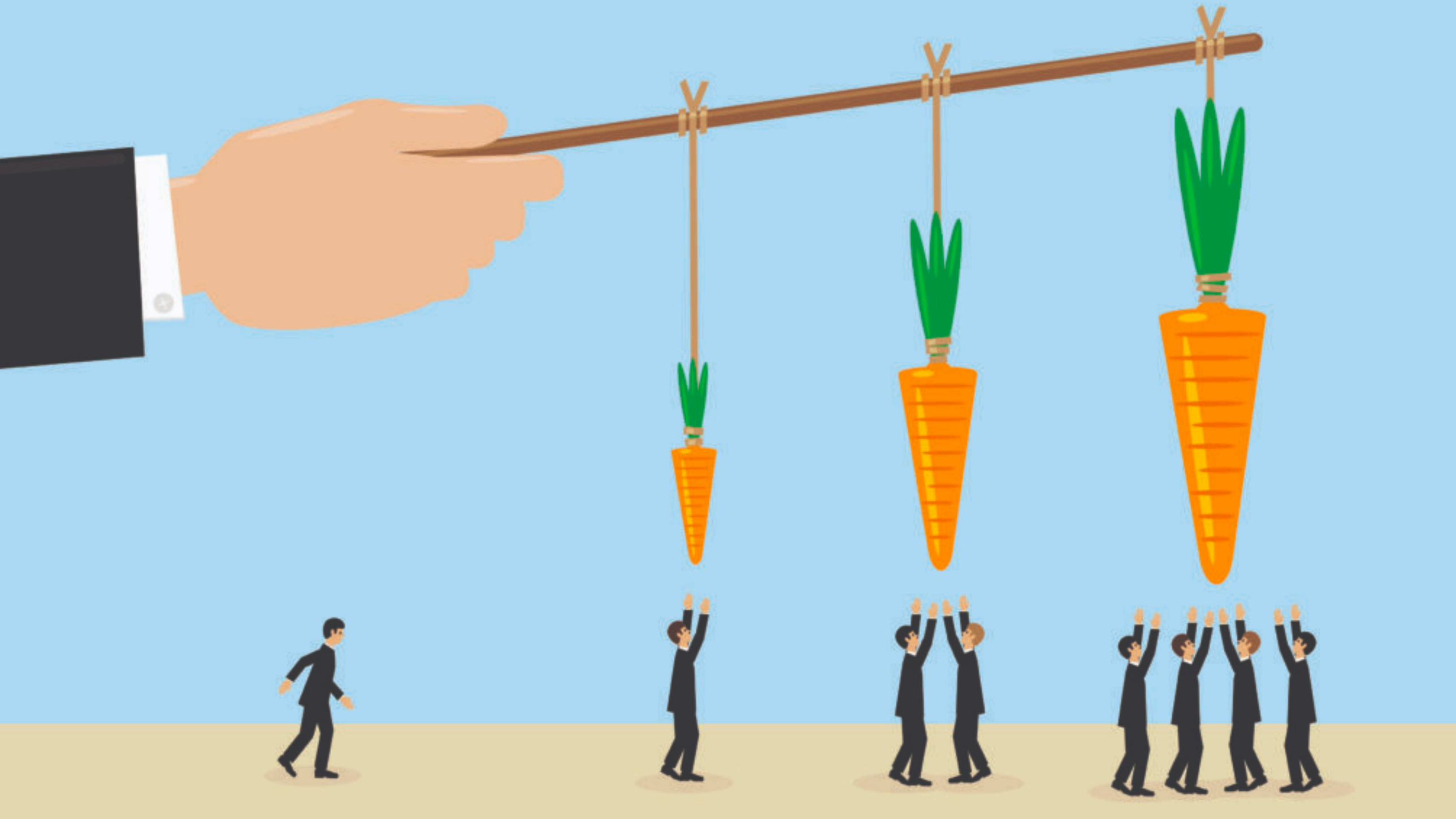
Collaboration

- Designed for Sen. Wyden's staff
- Based on Sen. Wyden' s (draft) legislation
- Works according to the legislation's constraints
- Prioritizes the legislation's needs and desired tradeoffs

Challenges: Reviewer #2

> The use of…MPC…demanded by the functionality of the system as a whole *is not very novel*. The authors use encrypted databases *in rather black-box ways*. I wonder if there is scope to *significantly strengthen* the paper to consider a narrower implementation of some of these primitives that are scoped only to this particular problem.

- What is the goal of this work?
  - use our expertise to solve a new technical problem that
    - experts asked us to solve…
    - …under the constraints they laid out…
    - …and based on assumptions that they vetted
  - *it is not to impress you (or anyone else) with how smart we are*



Challenges: Incentives

- No funding
  - 1 associate prof, 1 postdoc, 1 PhD student, 2 M.Sc. students
  - Took about 2 years

- Faculty only get paid for 9 months of out of 12…
  - …and need funding for 3 months of salary & to support PhDs & postdocs

- Funding sources
  - National Science Foundation: few get it and focused on trendy areas
  - DARPA, IARPA, …: focused on government & military needs
  - Industry: focused on industry trends

Challenges: Incentives

- Protocol and system will likely never be used
  - National gun registry is a political 3rd rail
  - Legislation might never even come out
  - Timing is subject to political landscape

- Likely no opportunity to claim “real-world impact”
  - which helps for tenure and future funding

Challenges: Incentives

- Clear that our work would have
  - no industry impact
  - no financial impact
  - very unlikely to have any practical/real-world impact

- Hope it will have *policy* impact
  - Gun violence is one of the most important social problems in US
  - Gun control is one of the most intractable US policy problems
  - Privacy of gun owners is a crucial element in this debate
  - Maybe our work removes this concern & help change the debate?

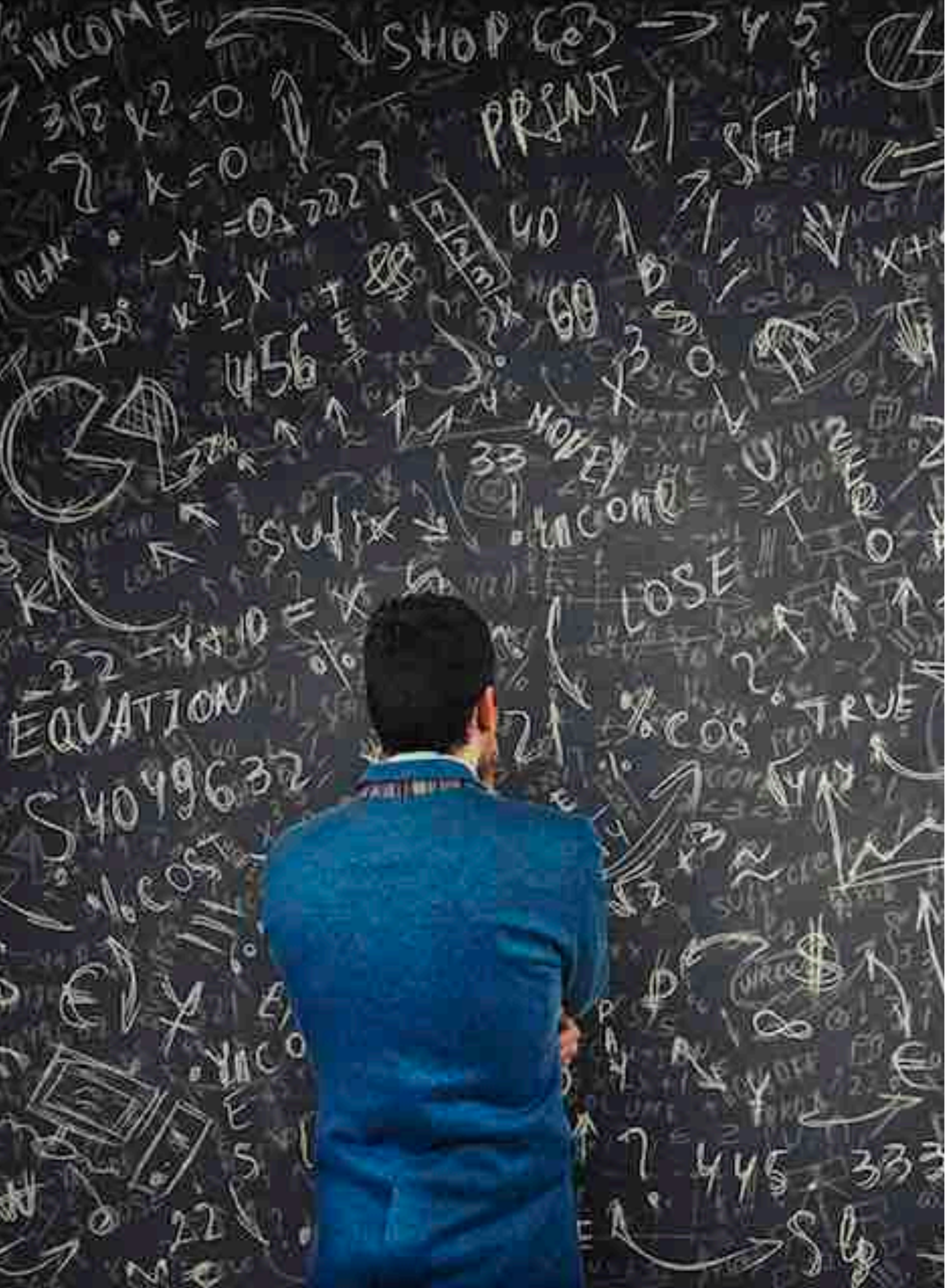
Education

- Since the 2000's
  - clear that technology is directly impacting *people*
  - ML & automated decision making, social networks, digital communication, erosion of privacy, …
- Different than the 60's-90's
  - technology's impact on people's lives was less direct
- But CS education hasn't changed

Education

- CS education
  - values STEM over everything else
  - prizes technical prowess over critical thinking
  - trains exclusively to solve quantitative problems

- Social problems
  - are not “well-posed” problems
  - do not have an optimal solution
  - span many fields that have nothing to do with STEM



Classical Computer Science Student

- Courses
  - intro to programming
  - OS, compilers, networking
  - algorithms, discrete math, complexity theory, cryptography
  - ML, AI, computer vision
  - Electrical engineering
  - Linear algebra, multivariable calculus, statistics, probability theory
  - Biology, Chemistry, …
- Projects
  - built their own OS
  - implemented a ZK SNARK protocol

“Critical” Computer Science Student

- Courses
  - The core STEM courses +

  - Ethnographic research methods
  - Introduction to social psychology
  - Methods of social research
  - History of capitalism
  - Modern genocide
  - From Freud to QAnon