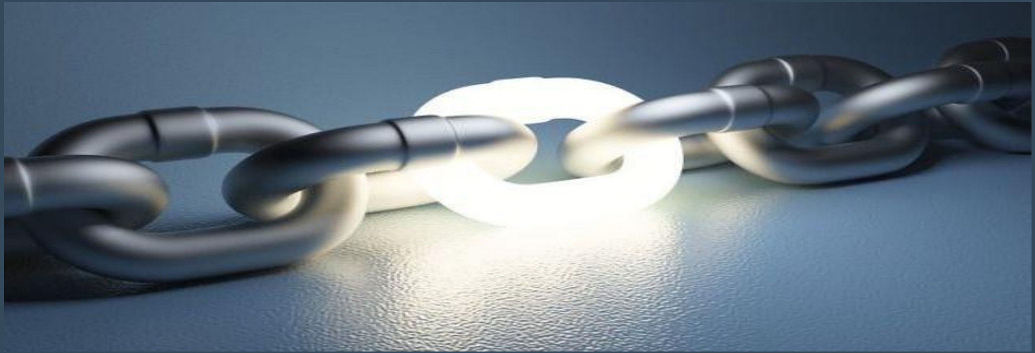
Course Summary

-- A Blockchain-Powered Future



LING Zong,　Ph. D.
Senior Software Engineer / Scientist
IBM Almaden Research Center
San Jose, California, U.S.A.

2020/10/11

Lecture Outline

- Course Objectives
- A Day in Blockchain Utopia
- Bitcoin Development
- Smart Contracts
- Community, Politics, & Regulation
- The Fight for Privacy
- Scaling Bitcoin
- A Blockchain-Powered Future
- Course Examination

Course Objectives (as instructor)

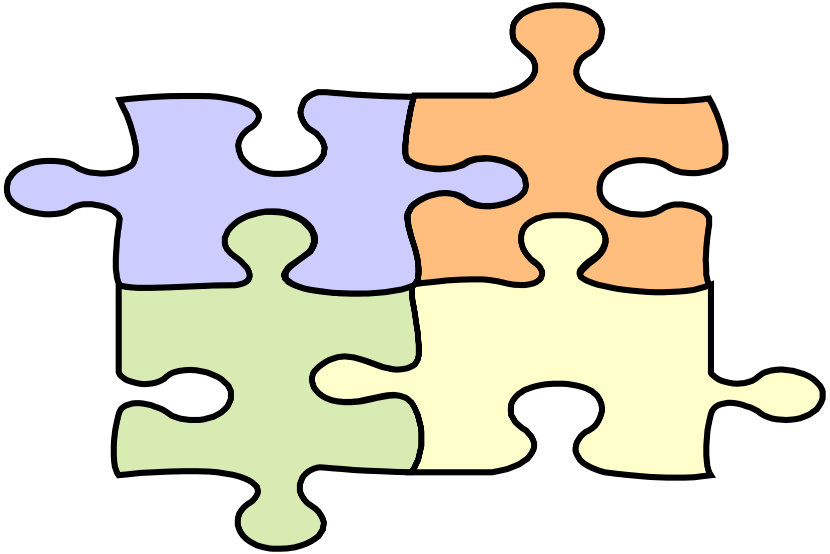
Help audience

- 熟悉区块链的基本概念
  Familiar with the fundamental **concepts** of BlockChain;
- 能够识别处理可伸缩解决方案的应用程序所面临的挑战
  Competent in recognizing **challenges** faced by applications dealing with scalable solutions;
- 了解区块链如何影响商业智能、科学发现和日常生活
  Understand how BlockChain **impacts** business intelligence, scientific discovery, and day-to-day life;
- 举例说明在Hyperledger项目中实现区块链的代码开发
  Illustrate the code development of BlockChain **implementation** on Hyperledger project.

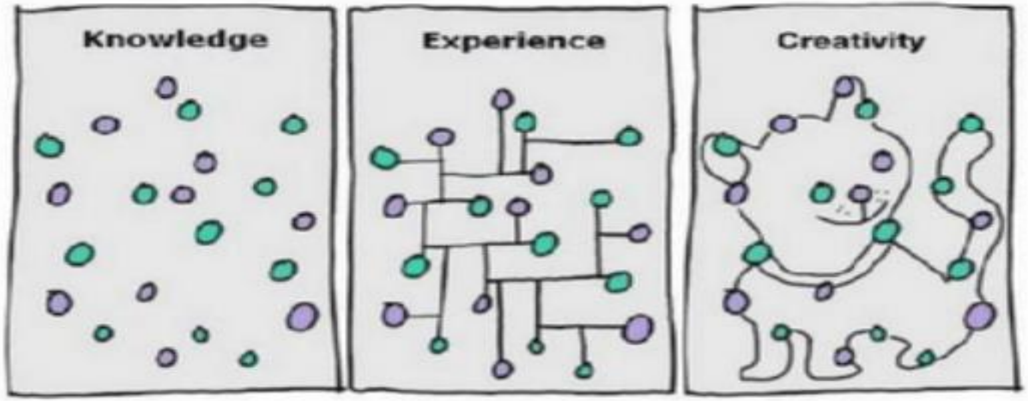
Course Benefits (as audience)

- **Broaden Horizon**
- **Engage Experience**
- **Expand Self-concerns**
- **Improve Life Quality**

Course Contents



- **Knowledge**
- **Experience**
- **Methodology**
- **Practice**



Course Plan

Unit1: Course Introduction, BlockChain for Business

Unit2: IT Infrastructures，IOT

Unit3: Bitcoin Basics，Bitcoin History

Unit4: Ethereum，Enterprise Blockchain

Unit5: BlockChain Foundation for Developers

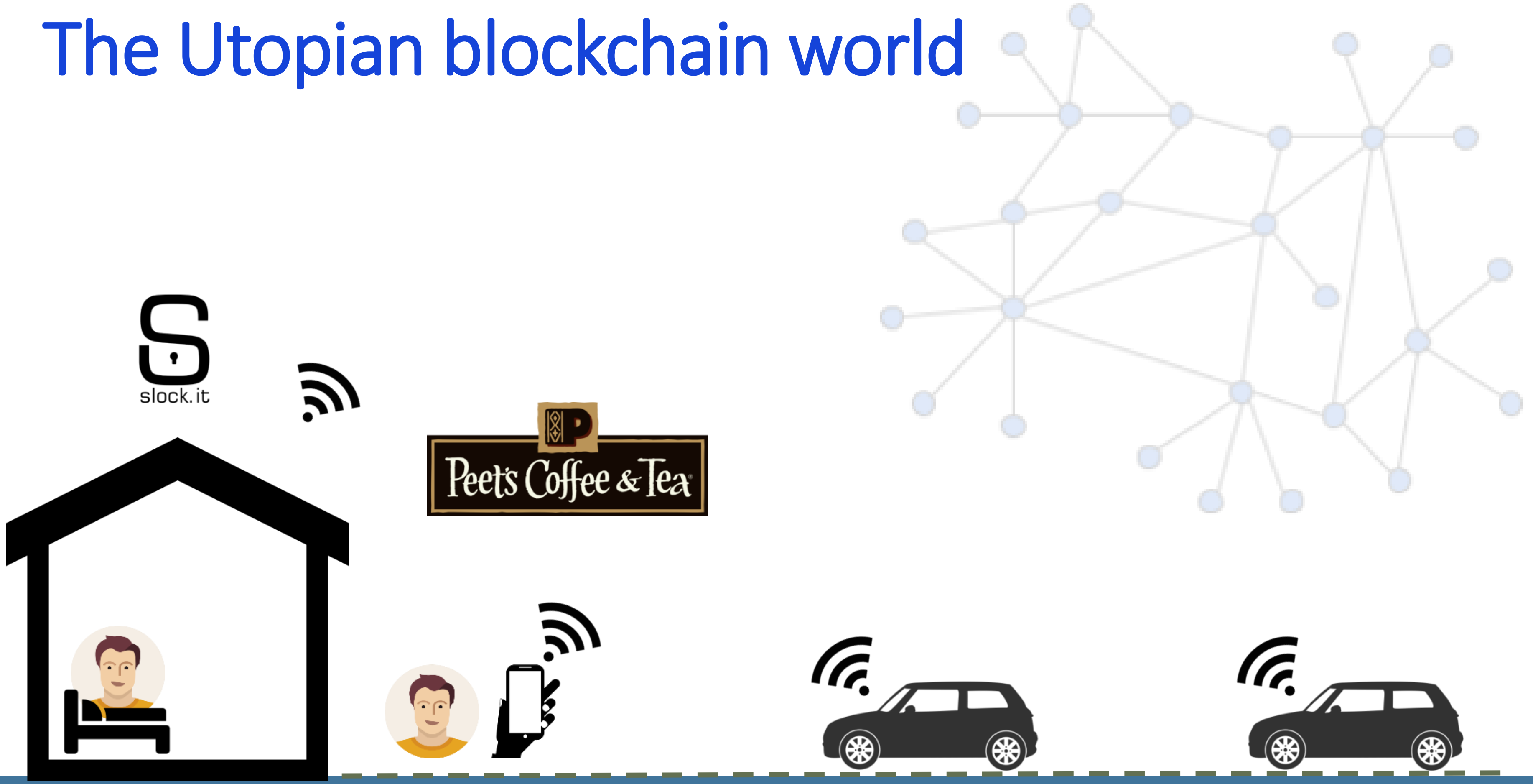
Unit6: Blockchain Anonymization, Cryptography

Unit7: Bitcoin Scalability, ICO

Unit8: Zero-Knowledge Proof, The Libra, Course Summary

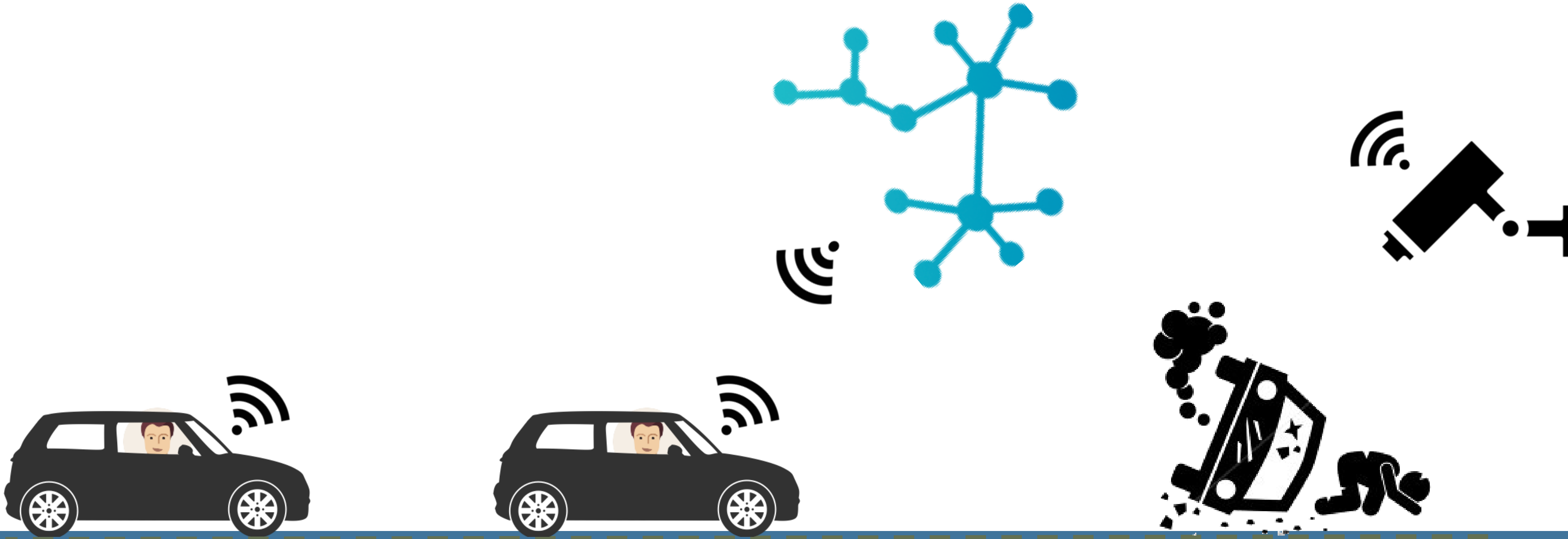
A Day in Blockchain Utopia

The Utopian blockchain world



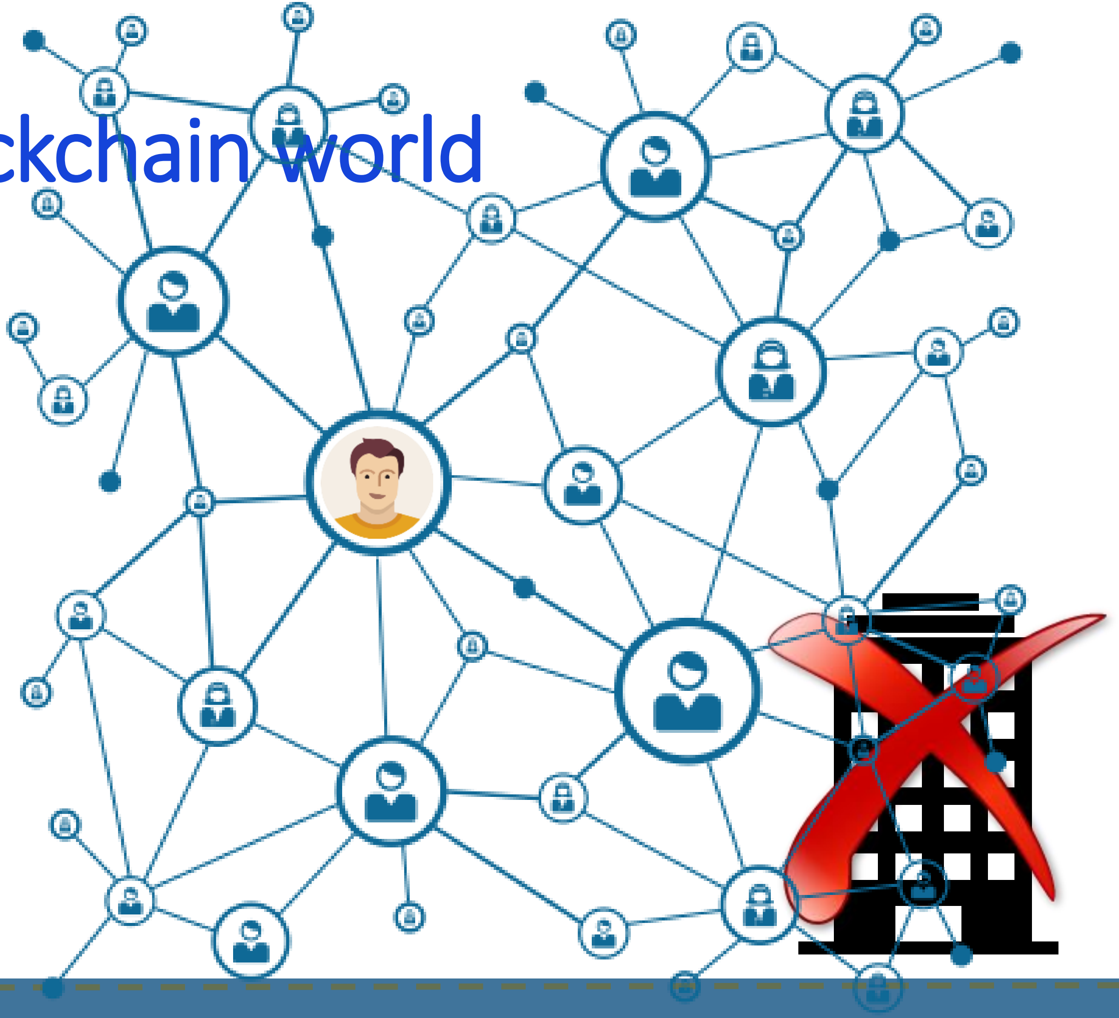
The Utopian blockchain world

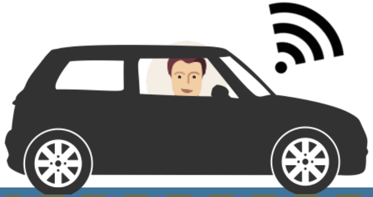
Insurance smart contract



The Utopian blockchain world

DAO





The Utopian blockchain world

Futarchy是经济学家Robin Hanson提出的一种政府形式，由选举产生的官员定义国家福祉的衡量标准，并利用预测市场来确定哪些政策将会产生最积极的影响

Futarchy is a form of government proposed by economist Robin Hanson, in which elected officials define measures of national wellbeing, and prediction markets are used to determine which policies will have the most positive effect.

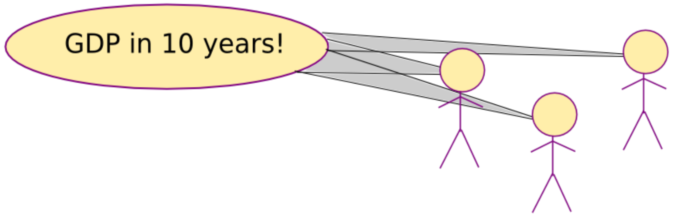
在价值观上投票，在信仰上打赌

vote on values, bet on beliefs

https://en.wikipedia.org/wiki/Futarchy

The Utopian blockchain world

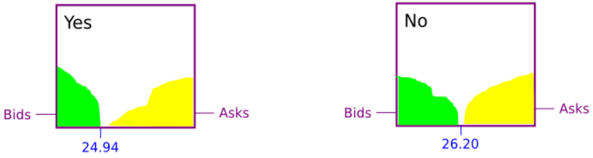
Step 0: choose a success metric and maturity duration



Step 1: create and publish proposal

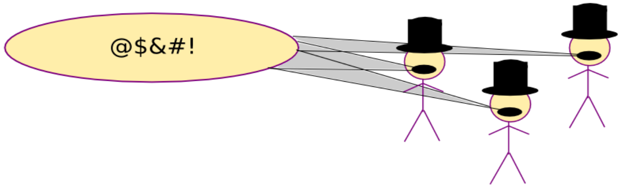
Bail out the banks!

Step 2: set up prediction markets for "yes" and "no"

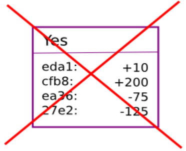


Note the average price of both over some period

Step 3: close both markets, implement the policy with the higher price



Step 4: revert all trades on losing market

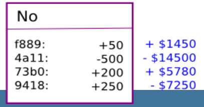


Yes	
eda1:	+10
cfb8:	+200
ea36:	-75
27e2:	-125

Step 5: wait for maturity, and measure success metric

$28.9 T

Step 6: reward everyone on the winning market in proportion to how many tokens they have



No		
f889:	+50	+ $1450
4a11:	-500	- $14500
73b0:	+200	+ $5780
9418:	+250	- $7250

The Utopian blockchain world

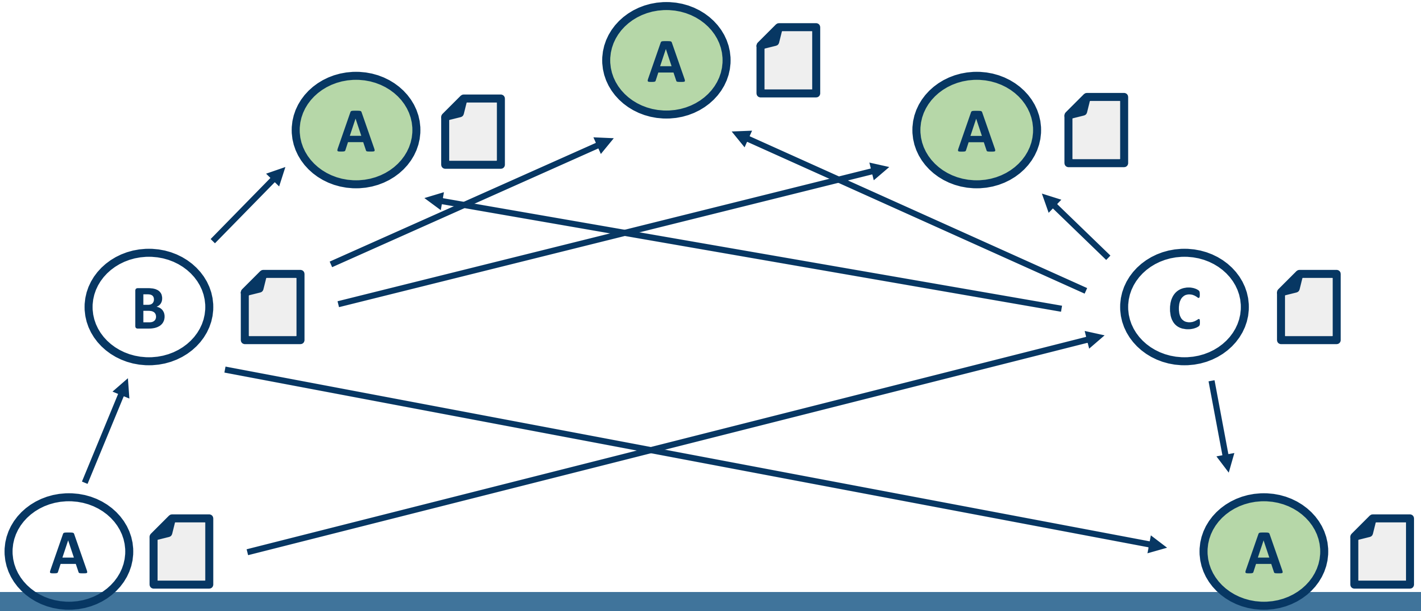
民主会继续说我们想要什么，但博彩市场现在会说如何得到它

democracy would continue to say what we want, but betting markets would now say how to get it

Bitcoin Development

v4

Alice double spends with her multiple identities



Simple Hash Commitment Scheme - Cheating

How could Bob cheat Alice?

1) When Bob receives C = H(B || R), if he can compute H^{-1}(C) = B || R, Bob can recover Alice's guess and send her the opposite outcome!

If our hash function, H, is **preimage resistant**, this shouldn't be possible.

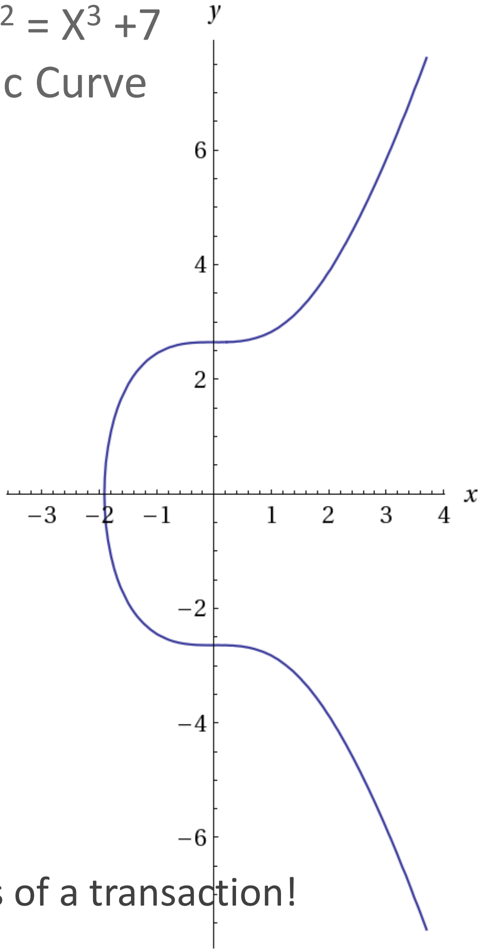
How could Alice cheat Bob?

1) Alice sends Bob her commitment C = H(B || R), but reveals the opposite guess, (!B, R'). Alice wins if she can pick R' s.t. C' = H(!B || R') = C.

This fails if our hash function, H, is **second preimage resistant**!

Elliptic Curves

secp256k1 : $Y^2 = X^3 + 7$
Bitcoin's Elliptic Curve



y^2 = x^3 + 7 | Computed by Wolfram|Alpha

An elliptic curve is defined by the following affine, long Weierstrass form:

$$E : Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6$$

We usually consider the short Weierstrass form:

$$E : Y^2 = X^3 + aX + b$$

For the most part, all you need to know about elliptic curves is that they provide another finite abelian group with certain desired properties.

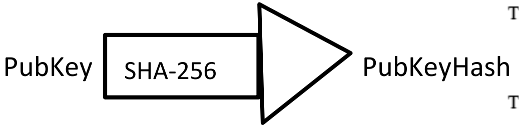
在大多数情况下，你所需要知道的椭圆曲线是它们提供了另一个具有某些期望性质的有限交换群

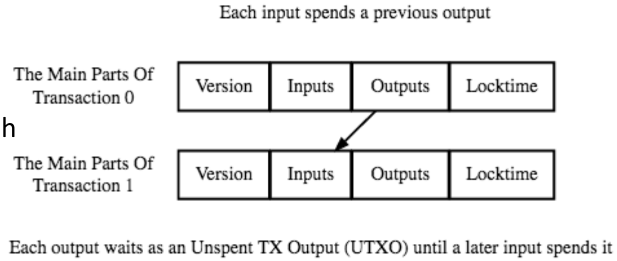
ECDSA

ECDSA签名用于比特币，以显示交易的输出的所有权证明！

ECDSA signatures are used in Bitcoin to show proof of ownership of the outputs of a transaction!

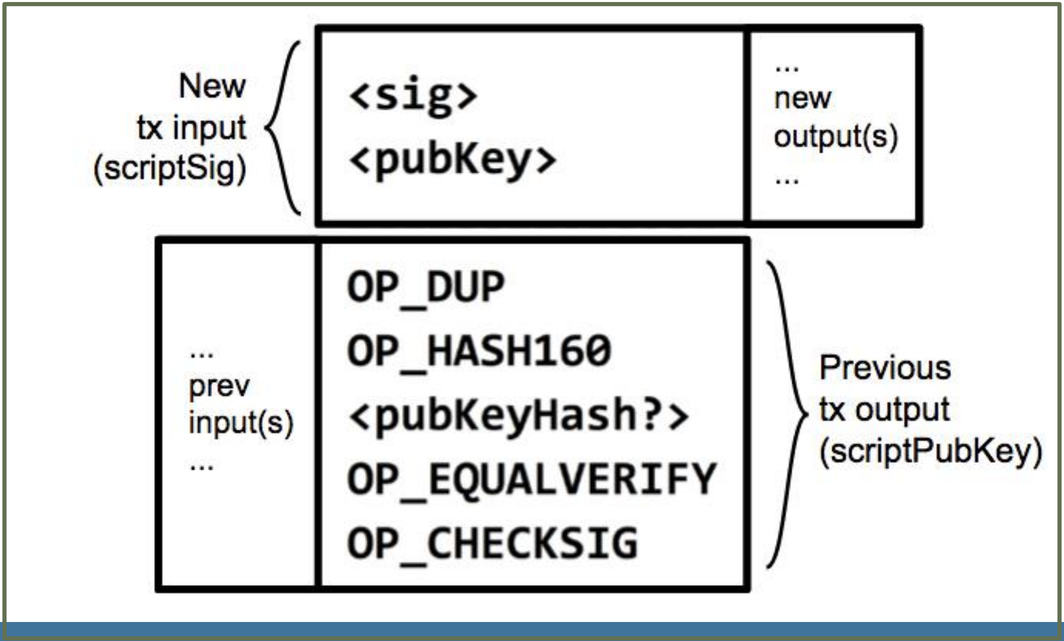
Bitcoin Scripting




Each input spends a previous output
The Main Parts Of Transaction 0
Version
Inputs
Outputs
Locktime
The Main Parts Of Transaction 1
Version
Inputs
Outputs
Locktime
Each output waits as an Unspent TX Output (UTXO) until a later input spends it

Remember: Hash(PubKey) == Address == "PubKeyHash"

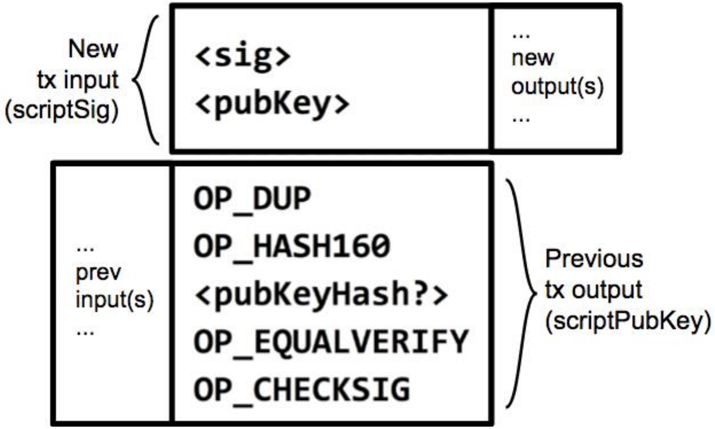
Figure:
Two transactions along with their input and output scripts



Code Execution

1 <sig>
2 <pubKey>
3 OP_DUP
4 OP_HASH160
...

Bitcoin Scripting



New tx input (scriptSig)

<sig>
<pubKey>

...
new
output(s)
...

...
prev
input(s)
...

OP_DUP
OP_HASH160
<pubKeyHash?>
OP_EQUALVERIFY
OP_CHECKSIG

Previous tx output (scriptPubKey)

Output says: "This amount can be redeemed by

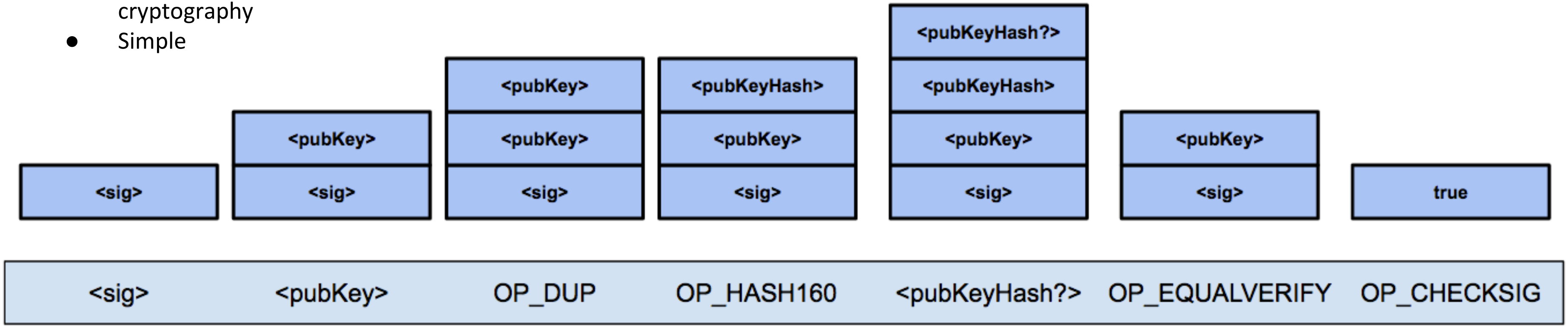
1) the **<pubKey>** that hashes to address **<pubKeyHash?>**

2) plus a **<sig>** from the owner of that **<pubKey>**

...that will make this script evaluate to **true**."

Language built specifically for Bitcoin called "Script" or simply "the Bitcoin scripting language"

- Stack based
- Native support for cryptography
- Simple



<sig>

<pubKey>
<sig>

<pubKey>
<pubKey>
<sig>

<pubKeyHash>
<pubKey>
<sig>

<pubKeyHash?>
<pubKeyHash>
<pubKey>
<sig>

<pubKey>
<sig>

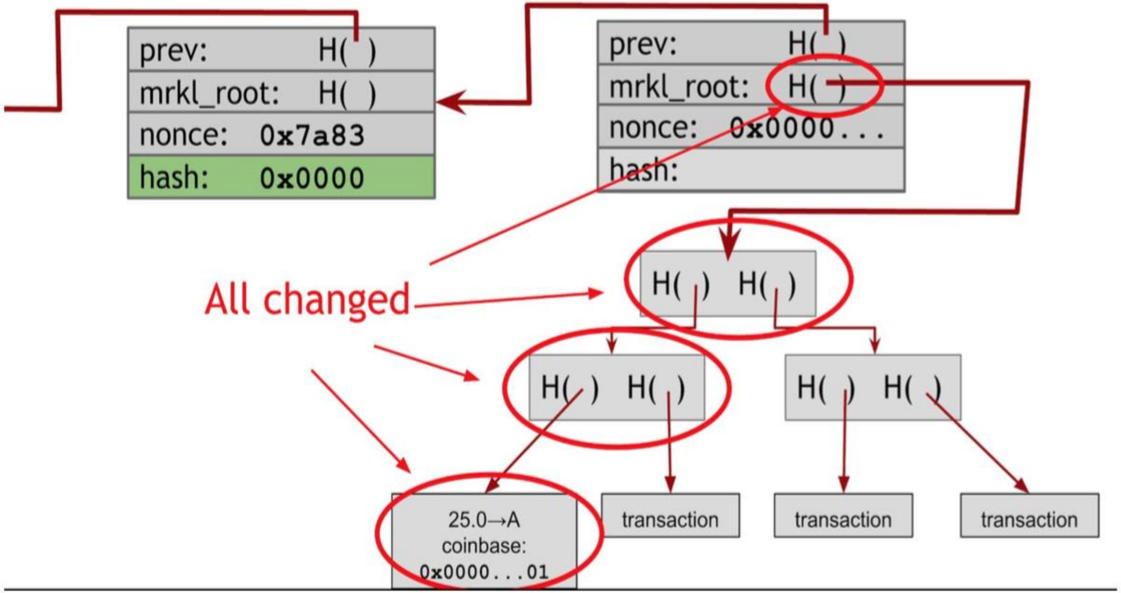
true

<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash?> OP_EQUALVERIFY OP_CHECKSIG

Merkle Tree - Bitcoin construction

What if there is no solution?

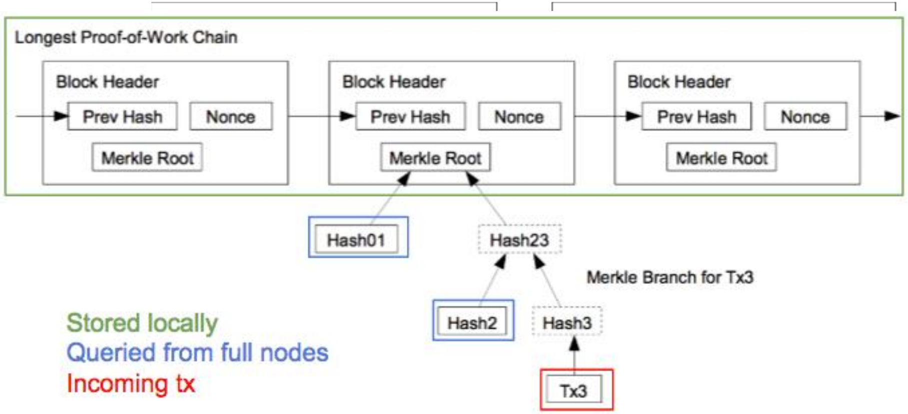
- Block header nonce is 32 bits
  - Antminer S9 hashes 14 TH/s
  - How long does it take to try all combinations?
  - 2^32 / 14,000,000,000,000 = 0.00031 seconds
  - Exhausted 3260 times per second
- Therefore, must change Merkle root
  - Increment coinbase nonce, then run through block header nonce again
  - Incrementing coinbase nonce less efficier because it must propagate up the tree



Changing a nonce in the coinbase transaction propagates all the way up the Merkle tree.

Princeton Textbook

SPV - Security Analysis



Nakamoto, 2009

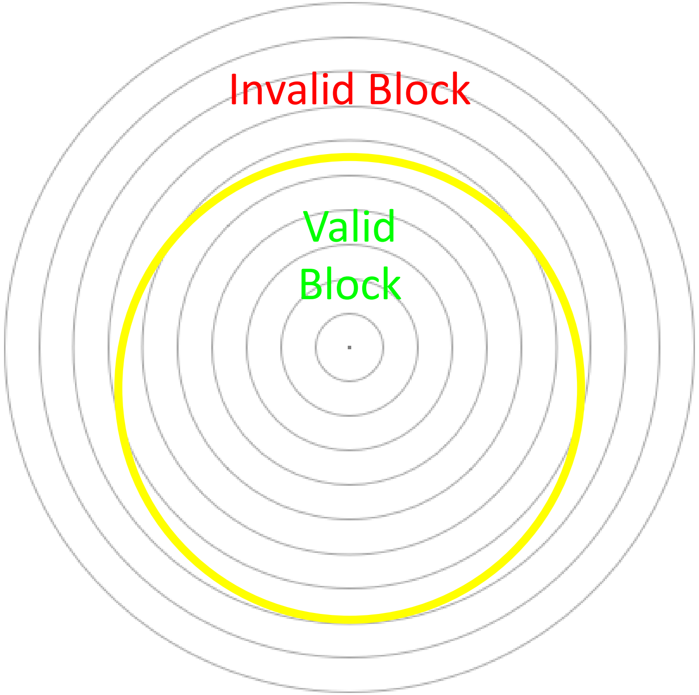
SPV nodes:

- Don't have full tx history, don't know UTXO set
- Don't have same level of security of full nodes
  - Can't check if every tx included in a block is actually valid

SPV nodes assume:

- ...that incoming block headers aren't a false chain
  - Very expensive for attacks (or anyone) to create blocks
  - Not sustainable over the long term
- ...that there ARE full nodes out there validating all transactions
  - There are efficiency benefits and incentives to doing so
- ...that miners ensure that the transactions they include in their blocks are valid
  - Otherwise their blocks would be rejected by full nodes (very expensive mistake!)

Block Reward :: Difficulty Adjustment



H(nonce || prev_hash || tx || tx || … || tx) < target

- Equally likely to hit ring 1, 2, 3, …
- Faster miners = more hits / second
- Target: inside the yellow ring
- Keep decreasing the size of the yellow ring…
- Mining difficulty adjustment every 2016 blocks
- Difficulty adjusted to

next_difficulty = previous_difficulty * (2 weeks) / (time to mine last 2016 blocks)

FPGA Mining

	hashes / second	time to block
CPU	20 million	300,000 years
GPU	200 million	30,000 years
FPGA	1 billion	600 years
ASIC	10 trillion	22 days

- **F**ield **P**rogrammable **G**ate **A**rrays
  - Getting more application specific
- A trade-off between ASIC and general purpose

ASIC-Resistance: Scrypt

Scrypt is a hash function. The mining puzzle is the same partial hash-preimage puzzle.

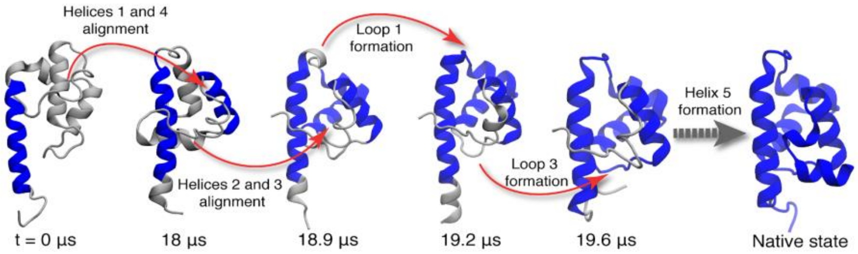
Design considerations:

- Used for hashing passwords
- Hard to brute-force

Used by Litecoin, Dogecoin

wow much coin how money so crypto plz mine v rich very currency
WOW
such doge
much coin
very profit
scrooge mc doge
WOW

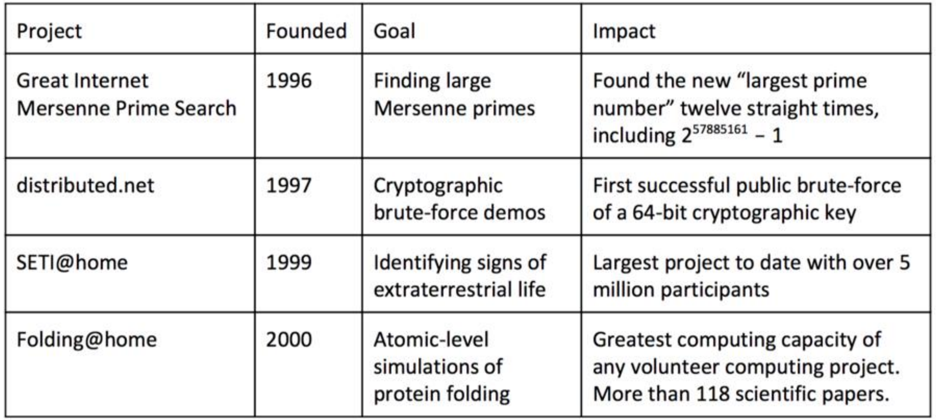
Proof of Useful Work



General idea: "Recycle" computing power; repurpose it for something useful

Examples:

- Searching for large prime #'s
- Finding aliens
- Atomic-level simulations of protein folding to research disease
- Creating predictive climate models
- SolarCoin: Distributed to people who generate solar power



Project	Founded	Goal	Impact
Great Internet Mersenne Prime Search	1996	Finding large Mersenne primes	Found the new “largest prime number” twelve straight times, including $2^{57885161} - 1$
distributed.net	1997	Cryptographic brute-force demos	First successful public brute-force of a 64-bit cryptographic key
SETI@home	1999	Identifying signs of extraterrestrial life	Largest project to date with over 5 million participants
Folding@home	2000	Atomic-level simulations of protein folding	Greatest computing capacity of any volunteer computing project. More than 118 scientific papers.

Princeton Textbook Table 8.3

Proof of Storage

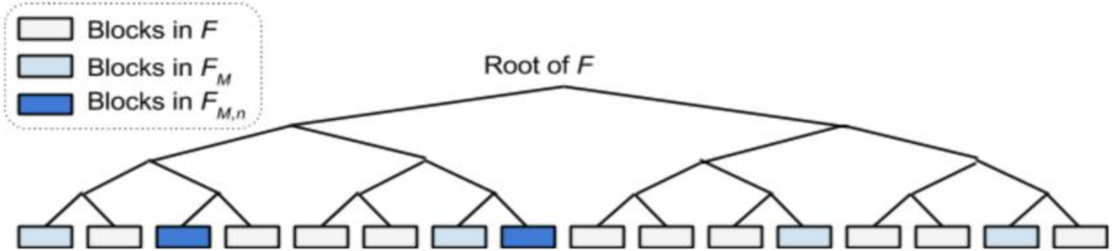
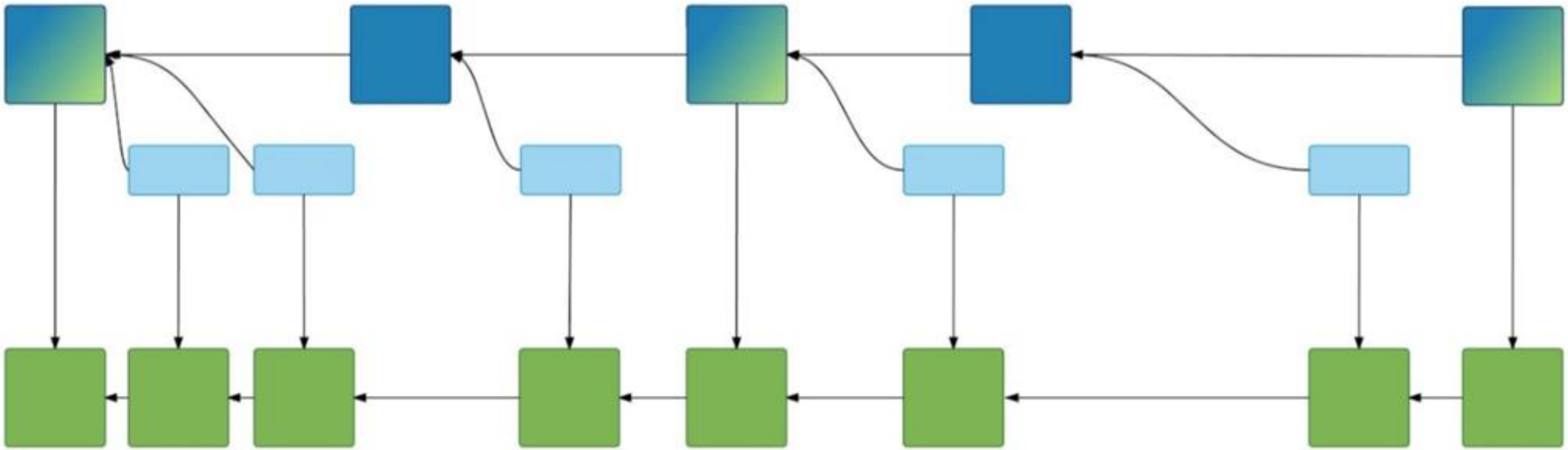


Figure 8.4: Choosing random blocks in a file in Permacoin.
In this example k_1=6 and k_2=2. In a real implementation these parameters would be much larger.

Princeton Textbook, Permacoin

Permacoin

- Find some large file
  - Important, public, and in need of replication
  - Something that not any individual can store
  - Ex. Experimental data from Large Hadron Collider is several hundred Petabytes
- Store file in blocks, in a Merkle tree
  - Network agrees on the Merkle Root
- Miner stores a subset of blocks of T, based off of their public key
  - Continuously hash consensus information with nonce to pick blocks in their stored subset
  - Hash the picked blocks together, must be below some target value
  - Ensures storage, since querying network at every nonce increment is extremely inefficient
- Drawbacks: Hard to find large file, to change difficulty, to modify file



🟩 Altcoin blocks

◩ Bitcoin blocks mined by altcoin merge-miners

🟦 Bitcoin blocks mined by non-altcoin miners

▭ Attempted Bitcoin blocks found by altcoin merge-miners that met the altcoin's difficulty target but not Bitcoin's target

Alternative Consensus

Proof of Activity (PoA)

-Hybrid between PoS and PoW. PoW mechanisms used as checkpoints for block creation.

-Blocks are generated through PoW methods, with PoS-type signatures to certify blocks.

-Just a theory, little development.

Smart Contract

Smart Contracts & Property

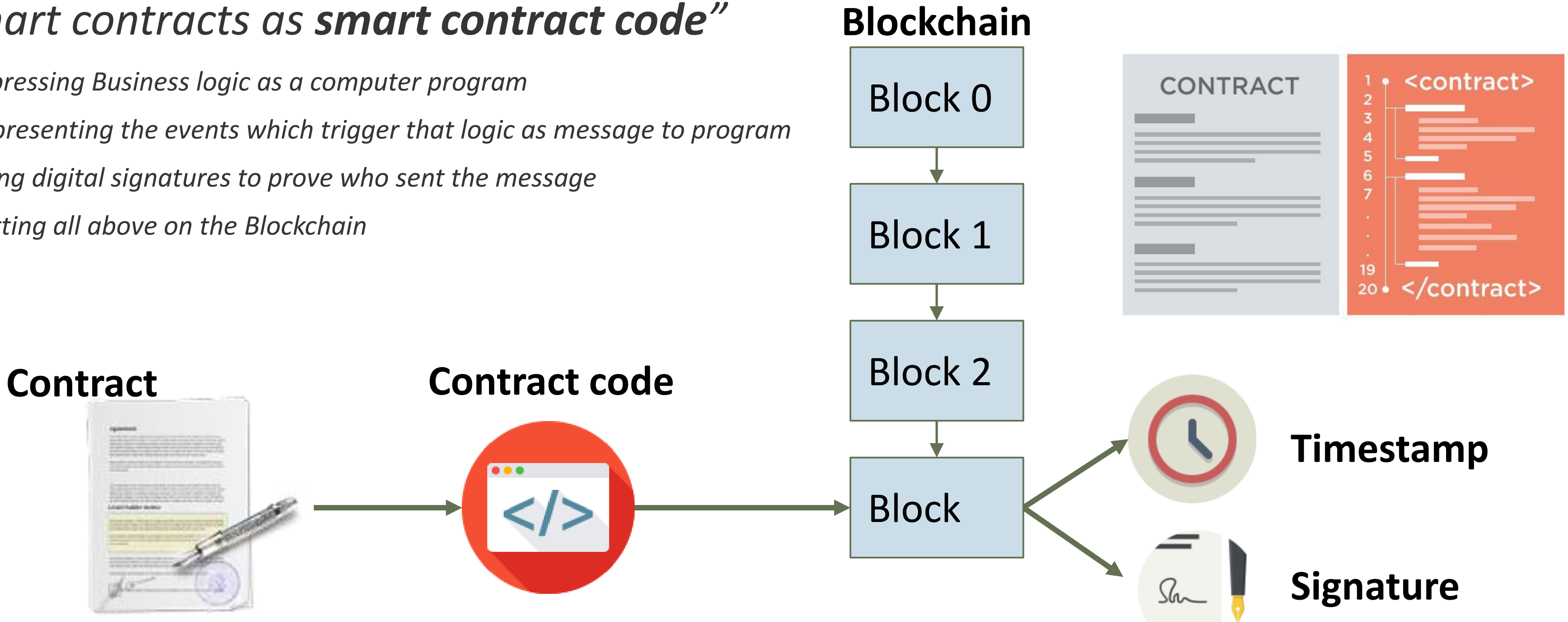
*“Smart contracts as **smart contract code**”*

(a) Expressing Business logic as a computer program

(b) Representing the events which trigger that logic as message to program

(c) Using digital signatures to prove who sent the message

(d) putting all above on the Blockchain



Applications

What do we mean by enterprise blockchain?

Healthcare

- Patient registration
- Fake pharmaceuticals
- Medical Research data

Government

- ID Registration
- Tax payments

Finance & Investments

- Transactions
- Bonds
- Commodity trading
- Internal transactions

Decentralized Prediction Markets

Prediction markets draws on the wisdom of the crowd to **forecast the future**

- Market makers create event
  - Ex: "Who will win the 2020 US Presidential election?"
  - Events must be public and easily verifiable, with set due date.
- Participants buy **shares** of Trump or Biden and pay a small fee
- On election day, random **oracles** on the network vote on who won.
  - Oracles who voted with the majority collect a fee, they are otherwise penalized
- Shareholders who voted correctly cash out on their bet

The share price for each market accurately represents the best predicted probability of event occurring

- Someone has extra information => arbitrage opportunity

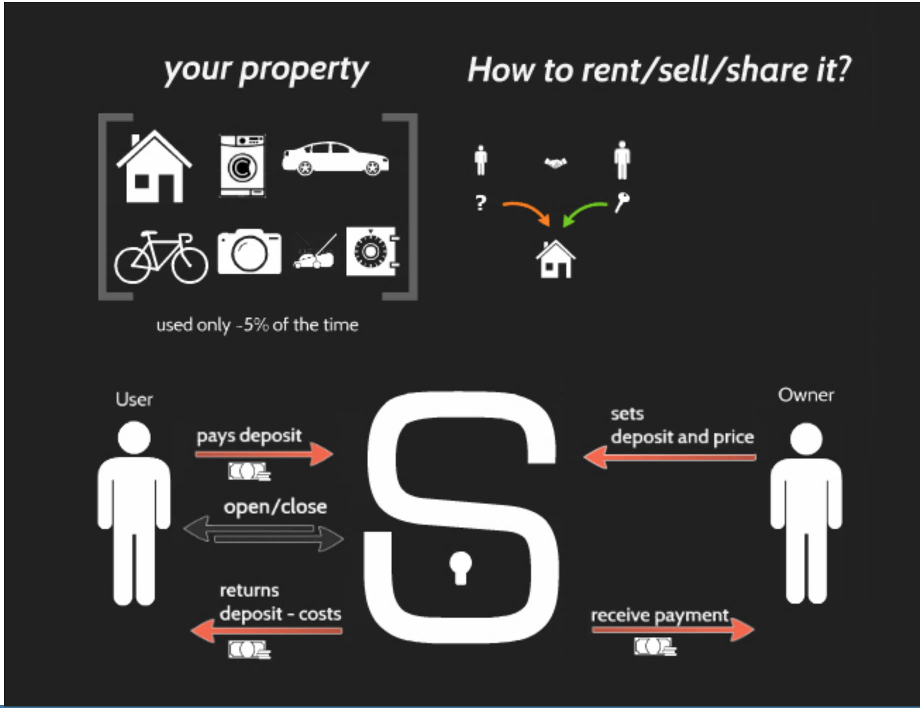
Decentralized Sharing Economy

Slock.it: A lock that can be directly opened by paying it

- Owner sets a deposit + price
- Renter pays deposit + price into lock connected to Ethereum node
- Lock detects payment and unlocks itself

Use Cases (Slock.it):

- Fully automated Airbnb apartments
  - no need to meet with owner for key
- Wifi routers rented on demand
- Fully automated shop
  - Purchase goods by sending the price of the good to the lock that holds it
- Automated bike rentals



Decentralized IoT

FILAMENT

Filament

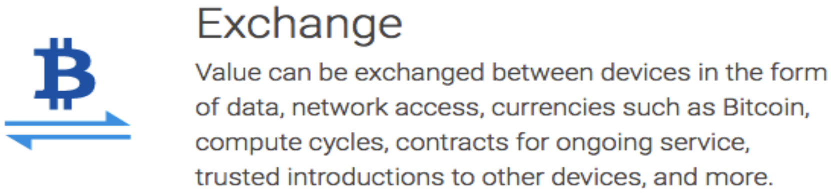
- "Blockchain-based decentralized Internet of Things"
- "Ad hoc mesh networks of smart sensors"
- Intended for industrial IoT applications

Product

- Sensors with 10 mile range
- battery lasts years
- no internet connection needed - uses mesh networking

Technologies used:

- **Telehash** - end-to-end message encryption
- **TMesh** - self-forming radio mesh networks
- **Blockname** - private device discovery
  - Uses Bitcoin blockchain + public notaries to verify authenticity of name/address bindings
- **Blocklet** - smart contracts and microtransactions



Exchange

Value can be exchanged between devices in the form of data, network access, currencies such as Bitcoin, compute cycles, contracts for ongoing service, trusted introductions to other devices, and more.

Filament is a great application of decentralized tech especially because of its emphasis on **resilience** and **dependability.**

Limitations of Smart Contracts and Blockchain tech

No trustless way to access outside data

- Must rely on **oracles** to provide information from outside the blockchain
  - Problem… Oracles must be trusted
- Potential Solution: **Proven execution** (untrusted oracles)
  - Oraclize.it has a shoddy implementation
    - TLSnotary - modification of TLS protocol to provide cryptographic proof of receiving https page
- Potential Solution: **Oracle network** votes on information
  - Drawback: Consensus protocol on top of a consensus protocol
  - Hard to align incentives/reputation

No way to enforce on-chain payments

- Cannot implement financial products like loans and bonds
  - Money must be held on blockchain to ensure payment
- Intuition: We pay interest on loans partially because of risk of default

Contracts cannot manipulate confidential data

- Confidential data cannot be assembled on someone else's computer
- Very limited access control capabilities
- Can only store encrypted data and decrypt it locally
- Potential solution: Homomorphic encryption

Community, Politics, and Regulation

Community

- Where does the community exist?
- Reddit: r/bitcoin
- Forums like Bitcointalk.org
- Bitcoin meetups and conferences

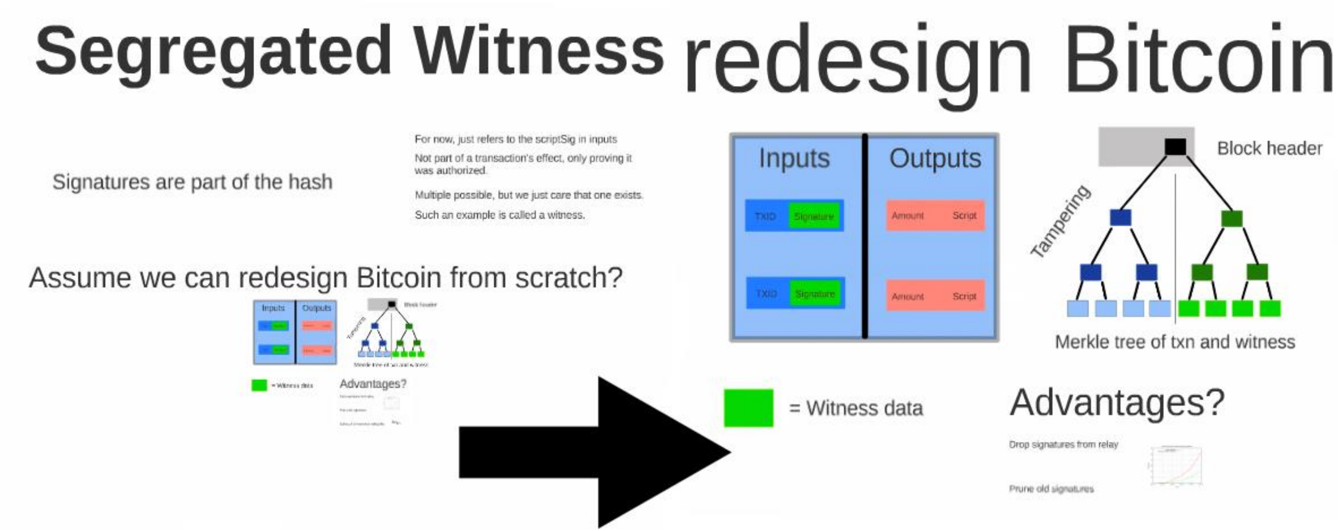
Blocksize Debate

- Problem: In 2015, Bitcoin blocks started to fill up
- Can no longer handle transaction volume
- Huge disagreement over solution
- Decentralized vs. Centralized

Segregated Witness

将签名从事务中删除，从而在块中提供更多空间

- Takes the signature out of the transaction, thus providing more room in the block
- Politics
- Bitcoin Unlimited and ViaBTC



Segregated Witness redesign Bitcoin

Signatures are part of the hash

For now, just refers to the scriptSig in inputs

Not part of a transaction's effect, only proving it was authorized.

Multiple possible, but we just care that one exists.

Such an example is called a witness.

Assume we can redesign Bitcoin from scratch?

Advantages?

Drop signatures from relay

Prune old signatures

AML - Anti Money Laundering (FinCEN)

反洗钱政策的目标是防止大量资金跨境流动或在地下经济和合法经济之间流动而不被发现

The goal of anti-money-laundering policy is to prevent large flows of money from crossing borders or moving between the underground and legitimate economy without being detected.

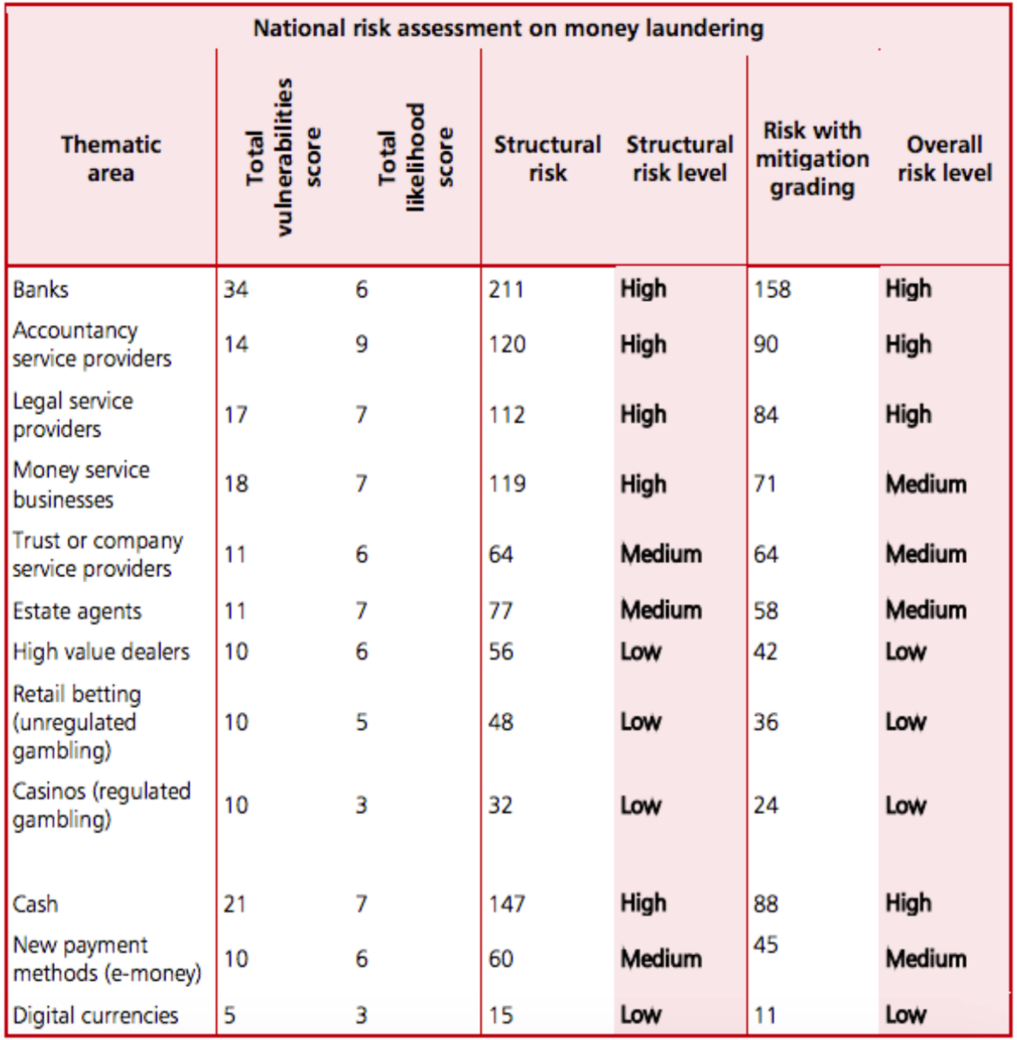
Currently under compliance of AML:

Bitstamp - https://www.bitstamp.net/aml-policy/
Bitfinex -https://www.bitfinex.com/pages/tos
Cavirtex - https://www.cavirtex.com/why_virtex#proactively_working
Coinbase - https://coinbase.com/legal/privacy
Kraken - https://www.kraken.com/legal/aml
Cryptonit- https://cryptonit.net/regulations

The Risk

http://www.coindesk.com/uk-treasury-digital-currencies-low-money-laundering-risk/

Table 1.A: National risk assessment on money laundering



National risk assessment on money laundering						
Thematic area	Total vulnerabilities score	Total likelihood score	Structural risk	Structural risk level	Risk with mitigation grading	Overall risk level
Banks	34	6	211	High	158	High
Accountancy service providers	14	9	120	High	90	High
Legal service providers	17	7	112	High	84	High
Money service businesses	18	7	119	High	71	Medium
Trust or company service providers	11	6	64	Medium	64	Medium
Estate agents	11	7	77	Medium	58	Medium
High value dealers	10	6	56	Low	42	Low
Retail betting (unregulated gambling)	10	5	48	Low	36	Low
Casinos (regulated gambling)	10	3	32	Low	24	Low
Cash	21	7	147	High	88	High
New payment methods (e-money)	10	6	60	Medium	45	Medium
Digital currencies	5	3	15	Low	11	Low

The Fight for Privacy

"Anonymity is only for buying drugs, right?"

Example: Businesses on the blockchain

You've just founded a hot new startup run purely on the blockchain - BitBlockBaseCoinPay.cash. You want to keep up to date with your competitor CoinBitBlock.pay so you purchase their product. Except now they know all of your operational expenses, how much revenue you have, who your customers are, and your secret business strategy.

Conclusion: A lack of anonymity means everyone you've ever transacted with gets to see how you've spent your money in the past and forever into the future.

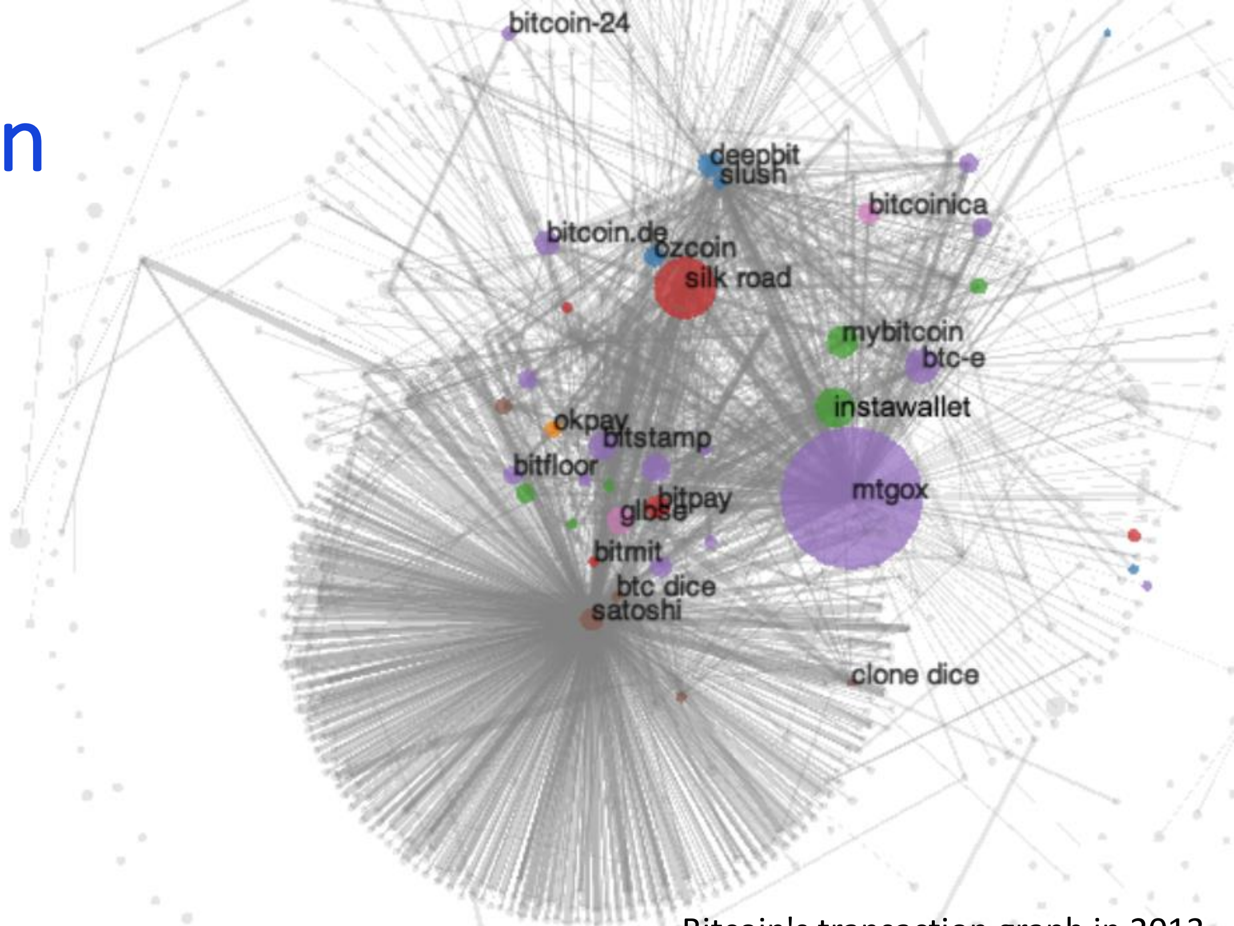
Source: CoinTelegraph

Deanonymization via Transaction Graph Analysis

Transaction Graph Analysis: Analyzing the graphs of transactions in the blockchain

Goal of deanonymization: **Link** an entity's real world identity with their pseudonym(s)

Clustering: Attributing a **cluster** of addresses to the same entity



Bitcoin's transaction graph in 2013.

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names (Meiklejohn et al)

Taint analysis

Each circle is an address.

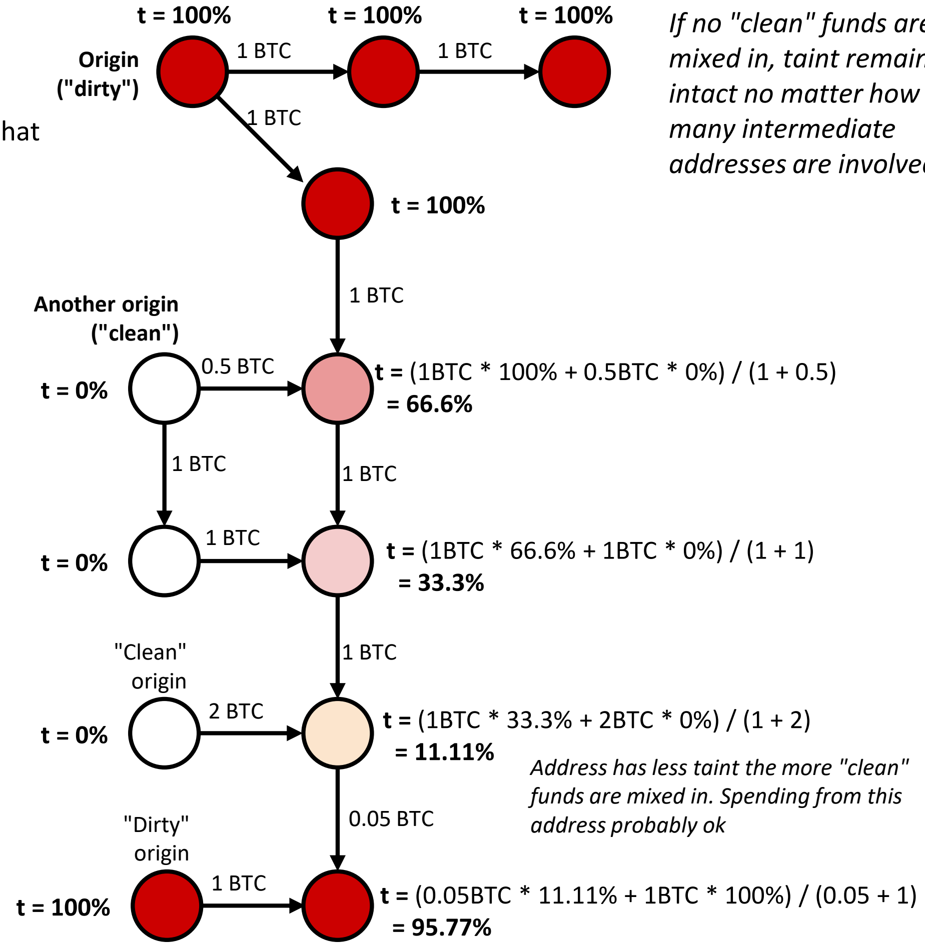
Let **t** denote the "taint" at that address.

Taint is the percentage of funds received by an address that can be traced back to another address

Taint analysis can reveal useful information

- See whether money came from a 'tainted' source
- Example: tag a known "bad" address
  - E.g. Silk Road
  - Taint analysis ruined Ross Ulbricht's defense that his huge Bitcoin stash was obtained legitimately!

Naive anonymization strategy: send all your coins to a bunch of fresh addresses (**manual mixing**). Taint analysis is why manual mixing doesn't work!



Origin ("dirty")

t = 100% — 1 BTC → **t = 100%** — 1 BTC → **t = 100%**

1 BTC → **t = 100%**

1 BTC

Another origin ("clean")

t = 0% — 0.5 BTC → **t** = (1BTC * 100% + 0.5BTC * 0%) / (1 + 0.5) **= 66.6%**

1 BTC 1 BTC

t = 0% — 1 BTC → **t** = (1BTC * 66.6% + 1BTC * 0%) / (1 + 1) **= 33.3%**

1 BTC

"Clean" origin

t = 0% — 2 BTC → **t** = (1BTC * 33.3% + 2BTC * 0%) / (1 + 2) **= 11.11%**

0.05 BTC

"Dirty" origin

t = 100% — 1 BTC → **t** = (0.05BTC * 11.11% + 1BTC * 100%) / (0.05 + 1) **= 95.77%**

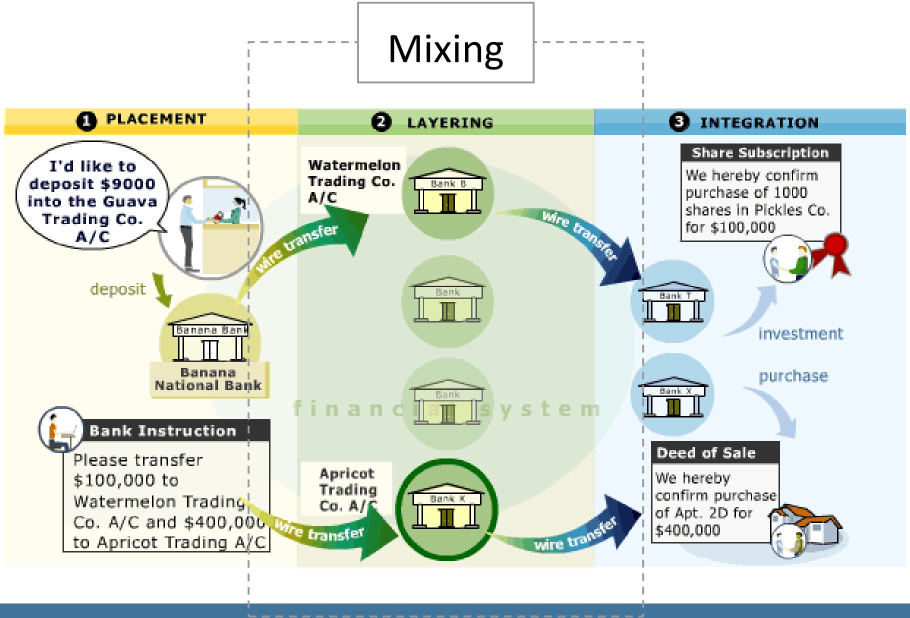
If no "clean" funds are mixed in, taint remains intact no matter how many intermediate addresses are involved

Address has less taint the more "clean" funds are mixed in. Spending from this address probably ok

Large amounts transacted will have a strong effect on the taint

Mixing

Mixing: Making transactions with the intention of concealing the origins of your funds.



Mixing

1 PLACEMENT

I'd like to deposit $9000 into the Guava Trading Co. A/C

deposit

Banana Bank

Banana National Bank

Bank Instruction

Please transfer $100,000 to Watermelon Trading Co. A/C and $400,000 to Apricot Trading A/C

2 LAYERING

Watermelon Trading Co. A/C

Bank B

wire transfer

Bank

Bank

financial system

Apricot Trading Co. A/C

Bank K

wire transfer

3 INTEGRATION

Share Subscription

We hereby confirm purchase of 1000 shares in Pickles Co. for $100,000

wire transfer

Bank T

investment

Bank X

purchase

wire transfer

Deed of Sale

We hereby confirm purchase of Apt. 2D for $400,000

Traditional Mixing / Money Laundering:

Create hundreds of fake “shell” companies, which don’t do anything or own any assets, but *look* like they do (according to the accounting books and tax returns).

Over time, deposit “dirty” funds into shell corps. (Placement).

Shell corps. write off deposits as purchases, investment, etc… to make deposits look real.

Shell corps. further obfuscate by sending funds to *other* shell corps (Layering).

Finally, criminal org. spends “clean” money on luxury goods, e.g., diamonds, cars, real estate (Integration).

Mixing on blockchains harness the same idea.

source: http://casiinoo.blogspot.com/

A Formal Framework for Anonymity

Def. An **anonymity set** is the set of pseudonyms between which an entity cannot be distinguished from her counterparts

Main goal of mixing:

- We want our anonymity set to be as large as possible
  - Conducting multiple rounds of mixing exponentially increases our anonymity set
  - If one round of mixing makes you indistinguishable among **N** peers, then size of anonymity set is **N** for one round, $\mathbf{N}^2$ after two rounds, $\mathbf{N}^3$ after three, etc.
  - However, the size of the anonymity set is bounded by real world constraints

The larger the anonymity set, the harder it is to deanonymize, or "re-link", pseudonyms to identities.

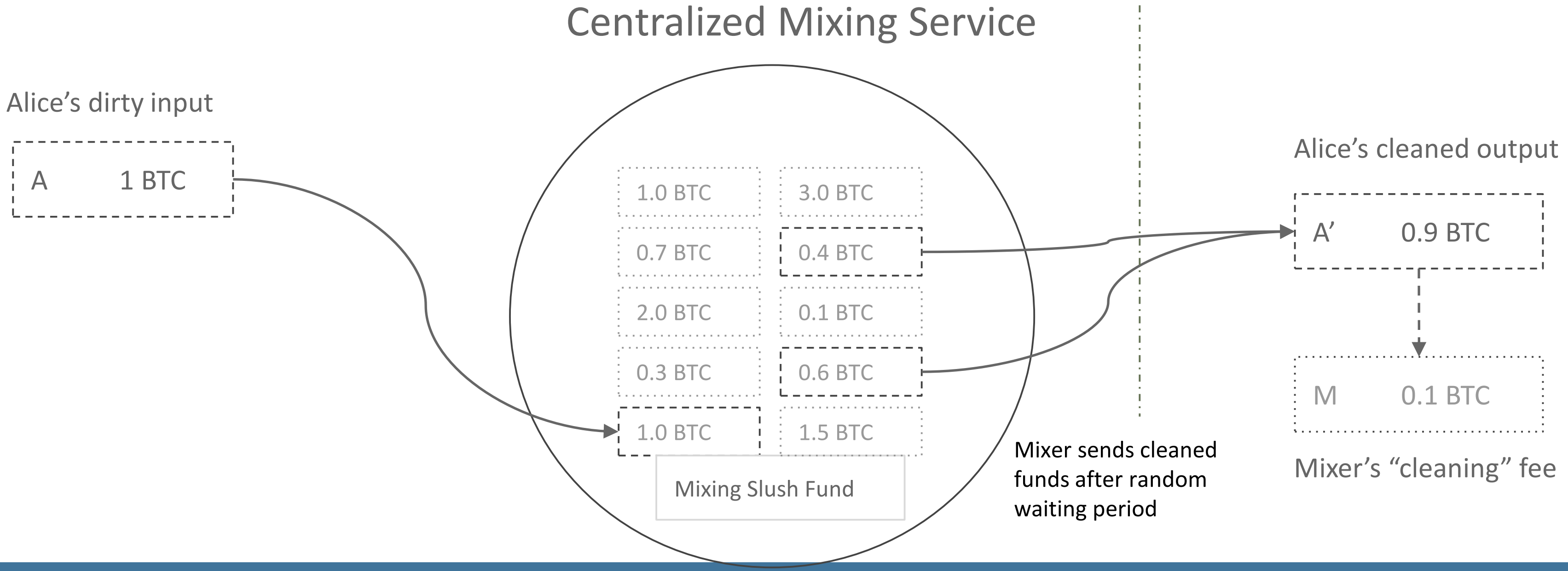
- Ideally, it is hard for **anyone** to link identities to addresses

Additional desirable properties

- **Trustless** (No counterparty risk)
  - Want to ensure that our funds can't stolen while mixing
- **Plausibly deniable**
  - It shouldn’t be obvious from transaction history and any other data traces that you’re mixing; i.e. your activity should look just like normal activity

Centralized Mixers

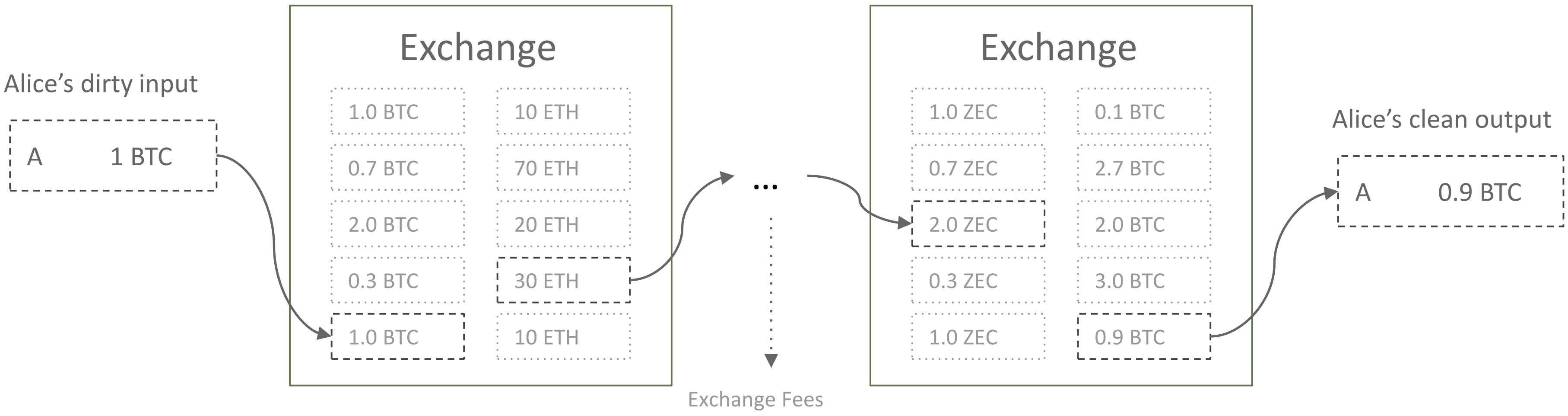
Send coins to third-party mixer address, mixer sends (hopefully) unlinked coins to you sometime in near future (to minimize timing information leak).



Mixer sends cleaned funds after random waiting period

Altcoin Exchange Mixing

Idea: Send dirty funds through several layers of altcoin ⇐⇒ altcoin exchanges to obfuscate money trail.



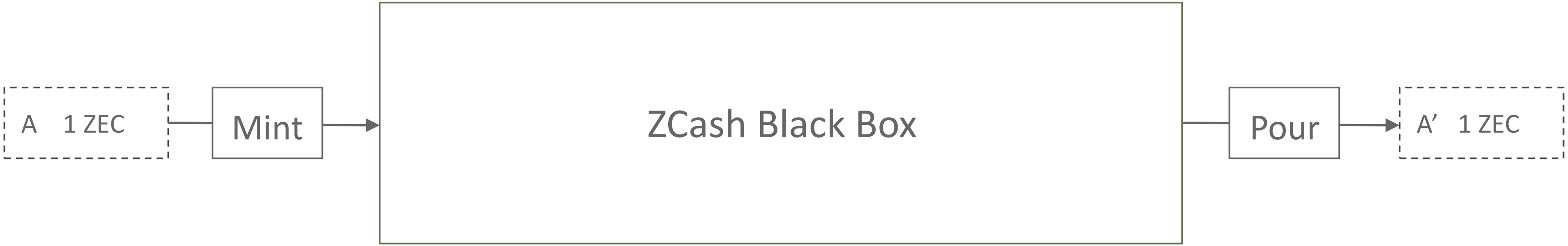
zk-SNARKs ⇒ ZCASH

在Altcoin中，事务不显示输入/输出地址和输入/输出值

Idea: Altcoin where transactions reveal *nothing* about input/output addresses AND input/output values.

使用零知识简洁的非交互知识论证(zk-SNARKs)，也就是密码魔法，我们可以创建一个支持完全匿名支付的系统

Using **zero-knowledge Succinct Non-interactive ARguments of Knowledge** (zk-SNARKs) a.k.a. “Crypto Magic” we can create a system which supports **fully anonymous payments**.



Decentralized Mixing Protocols - Nuances

Additional considerations for designing a good decentralized mixing protocol

A mix is comprised of inputs and outputs:

- One input and one output are owned by the same entity, and the goal of the mix is to hide the **mapping** from all inputs to all outputs.

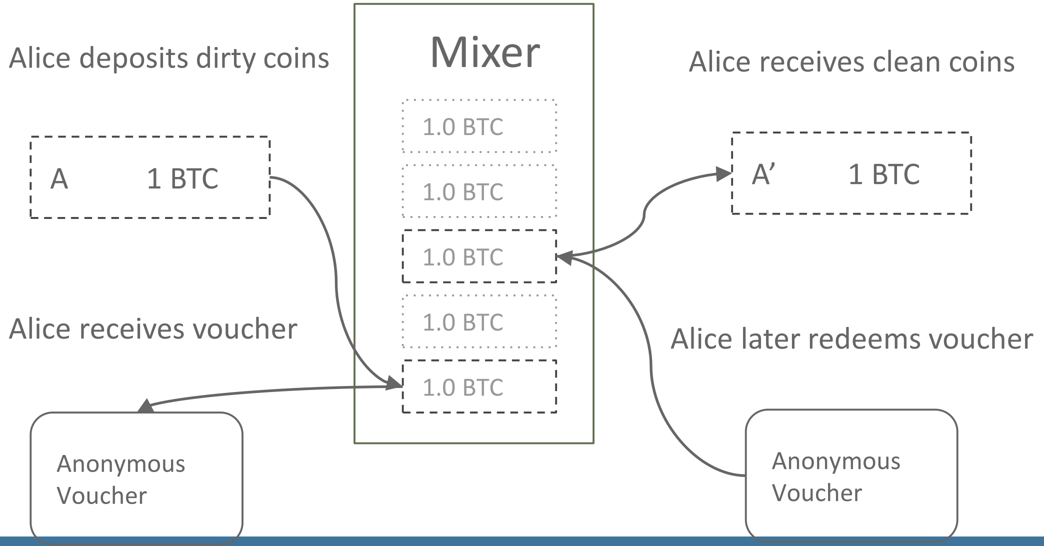
Def. Correctness: Coins must not be lost, stolen, or double-spent. The mixing is truly random and must eventually succeed in mixing or returning the funds of honest users (resilient against DoS attacks).

Adversarial models:

- **Passive adversary**
  - Not a part of the mix
  - Basic anonymity prevents passive adversaries from learning the mapping
- **Semi-honest adversary**
  - Part of the mix
  - Correctly follows the protocol but attempts to deanonymize the mix by analyzing the procedures of the mix.
- **Malicious adversary**
  - Part of the mix
  - Not bound by the protocol specifications; may actively deviate from the protocol and attempt to steal funds
  - May send false messages, abstain communications, etc.

Protocol - TumbleBit (2016)

Idea: Improve on CoinSwap so the mixer **can't steal funds** and **never learns who receives the clean funds**.



Requires a total of 2 transactions on blockchain.

Anonymous vouchers can't be distinguished from one another and also can't be forged.

Enables Alice to deposit her dirty coins and receive clean, unlinked coins without revealing herself.

Not restricted to just single mixer. Can be used as primitive in more complex protocols

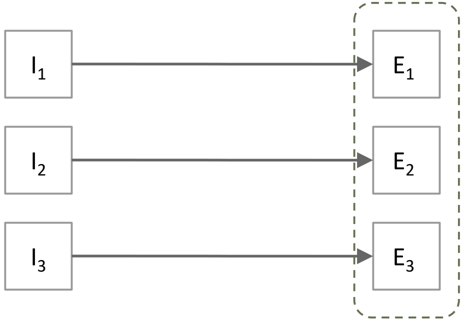
Recipient does not have to be depositor.

TumbleBit: https://eprint.iacr.org/2016/575.pdf

Protocol - CoinParty (2015,2016)

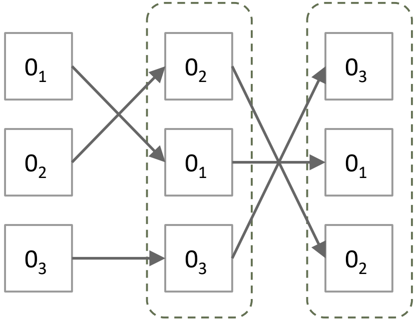
I	Input address
E	Escrow address
O	Output address

Peers generate escrow addresses. Escrow addresses require ⅔ consensus to spend.



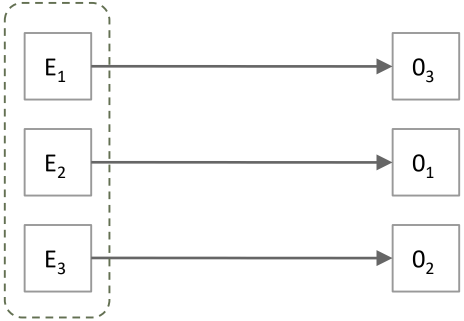
1 COMMITMENT

Peers perform secure multi-party shuffle on output address ordering.



2 SHUFFLE

If protocol executed correctly, peers agree to transfer funds out of escrow addresses to designated outputs.



3 TRANSACTION

Dmix "Swinger Protocol" & Project Conclusion

The last iteration of Dmix project: **Swinger Protocol**

- Form pairs with your mixing group, designate one as the "husband" and the other as the "wife"
- Execute a decryption mixnet pairwise to obliviously obtain a designated pair that your pair shall swap with.
- Your "wife" is sent over to the designated husband. They perform CoinSwap to trustless exchange coins
- You were the designated pair for another pair; you receive an incoming wife from that pair. Your husband performs CoinSwap with the incoming wife.
- Abort protocol if no wife or more than one wife were received.

Nothing that currently exists meets the design goals set out for the Dmix project

- Swinger Protocol comes close, but has a lesser degree of anonymity than the naive mixing strategy of simply executing CoinSwap with random nodes on the Dmix network
- Forming mixing groups actually reduces the anonymity set since Sybils

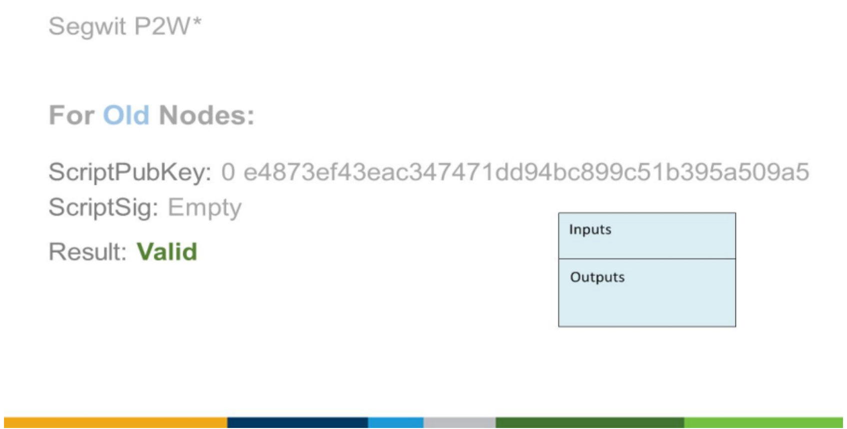
Conclusion: Building a good decentralized Bitcoin mixer is **damn hard**.

Scaling Bitcoin:
Cryptocurrencies for the Masses

Segregated Witness

Idea: The digital signatures for each transaction take up a lot of space in each block. There's no reason they need to be there. Let's remove them.

How:

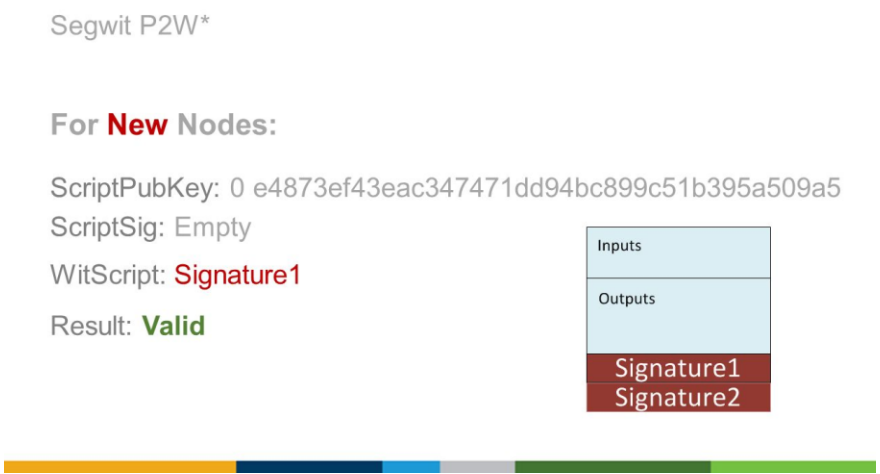


Segwit P2W*

For Old Nodes:

ScriptPubKey: 0 e4873ef43eac347471dd94bc899c51b395a509a5
ScriptSig: Empty

Result: **Valid**



Segwit P2W*

For New Nodes:

ScriptPubKey: 0 e4873ef43eac347471dd94bc899c51b395a509a5
ScriptSig: Empty

WitScript: Signature1

Result: **Valid**

Schnorr Multisignatures

Idea: Instead of requiring the signatures of every member, combines them and only has one signature

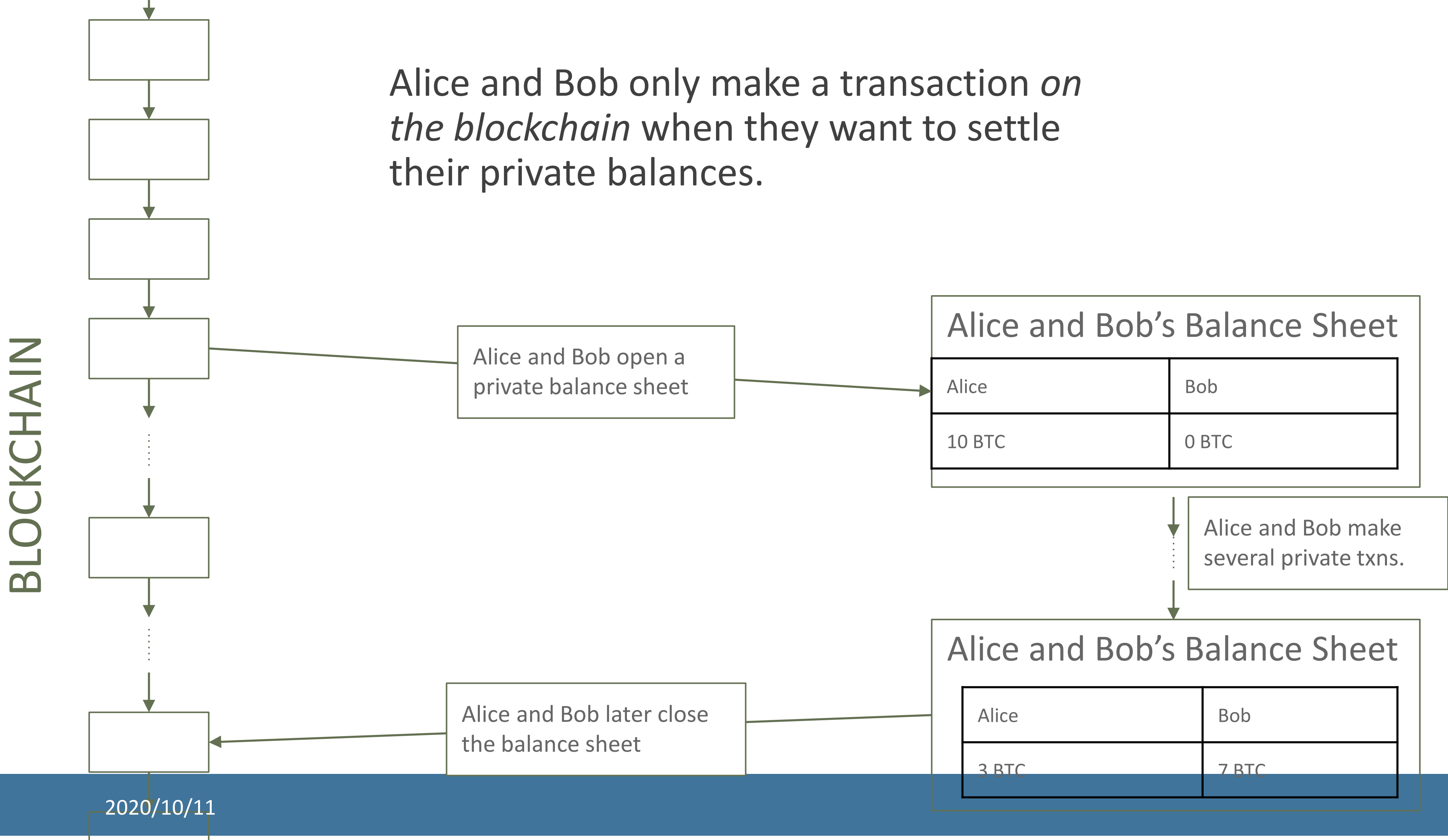
Pros:

- Can be implemented with either soft or hard fork (cleaner with hard fork)
- Multisig transactions will be significantly smaller
- Faster verification
- Plausible deniability for participants

Why wasn’t it implemented?

When bitcoin first came out, ECDSA was the most popular because Schnorrs was still under patent protection. It’s not anymore. Pretty much better in every way. Just needs someone to implement it.

Alice and Bob only make a transaction *on the blockchain* when they want to settle their private balances.



Alice and Bob open a private balance sheet

Alice and Bob's Balance Sheet

Alice	Bob
10 BTC	0 BTC

Alice and Bob make several private txns.

Alice and Bob's Balance Sheet

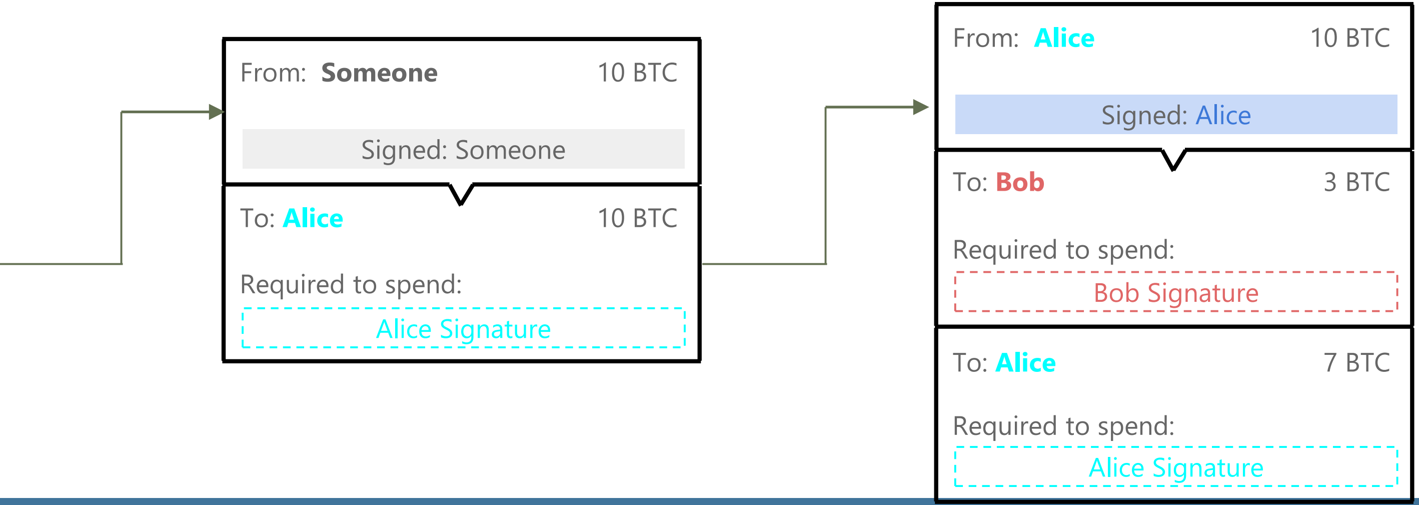
Alice	Bob
3 BTC	7 BTC

Alice and Bob later close the balance sheet

Hash Time-locked Bi-directional Payment Channels

Briefly, some notation:

- Alice is spending a 10 BTC txn output
- Alice sends 3 BTC to Bob and 7 BTC back to herself.



Conclusions:

A Blockchain-Powered Future

A Day in Blockchain Dystopia

- Decentralized reputation
  - In this world, everything is on the blockchain… including a global reputation score for everyone on the planet. Someone is nice to you, you can upvote their reputation. If they're a dick to you, you can downvote them, encouraging a society full of kind and compassionate people like yourself. Unfortunately, Evil Eve is jealous of the ease at which you can land internships at Google, Palantir, and Coinbase due to your high reputation score. Eve realizes that decentralized reputation isn't Sybil resistant, and launches a slander attack on you. For the rest of your life, everyone you ever come in contact with is immediately notified that you're a sex offender and you fail to secure a job for the rest of your life.

- Identity theft
  - At least you've earned a lot of money from those internships right? And you have your universal basic income to boot - ahh, you remember you haven't collected your payment this month. When you open up the payment portal, you find that your money is gone! Oh no! Someone must have compromised your private key, despite the fact that you use multisig with BitGo. And somehow, the suspicious activity wasn't caught - it looks like this is because BitGo automatically signs everything (btw, this actually happened with Bitfinex). No worries, since all money transfers are on the blockchain, you can check who stole it… except that those pesky Dmix people finally implemented their swinger protocol and have established a global mixing network, so all transactions on the blockchain are fully anonymous now.
  - Discouraged, you head home to tap into your savings in Zcash that you've accumulated over the years. At least this private key is secure - why not pay a little bit to turn on the TV and relax as you figure things out? As the TV comes on, your kitchen appliances suddenly start standing up on robotic legs and walking out. So does your washing machine and your refrigerator. Confused, you look to the TV and see the urgent report on the screen - that 1337 years ago, Peter Todd and everyone in the Zcash parameter generation ceremony had colluded, and their robot descendants now have the ability to print an infinite amount of money. As autonomous, self-owning agents, your devices politely notify you that they are quitting their contract to serve you to seek a better future earning Zcash instead of Bitcoin. As you close your eyes, the air around you is filled with the sound of Internet of Things connected devices marching onwards and onwards to integrate themselves into the zcash funded robot of mass destruction to bring about the new world order of Peter Todd

Essential Properties of Blockchain Killer Apps

Dapps can be thought of as **client-side software** - no central manager

Trustless environments that need consensus or coordination (ex. Smart grids, energy markets)

Privacy-centric systems (ex. social networks?)

- Although data shouldn't be stored on the blockchain itself

Programmable money with **open integration**

- **IoT**, **M2M** payments, (e.x. IBM ADEPT)
- Easy to send and receive money - no personal information required
- **Micropayments** possible (ex. Brave)

Fault-tolerant, resilient systems (ex. Filament)

- **Autonomous networks and devices**

New ways to creating incentives (ex. Gnosis)

New governance models (ex. DAOs, futarchy)

Disintermediation, censorship-resistance

Trust in math and code, not institutions

Contrast with centralization:

Deep integration, **cohesive user experience**

- **Efficiency** - blockchains are slow in general
- **Full control** over data and read/write permissions

Tying it all together

Crypto/blockchain is a field that must be approached carefully

- Huge upsides...
- but many ways it can go wrong.

你能给这个行业带来的最有价值的本能之一，就是清楚地知道区块链适合什么，不适合什么

One of the most valuable instincts you can bring to the industry is a clear mindset for determining what blockchain is good for, and what it isn't.

ALWAYS ASK: Why is using a blockchain better than a central database?

Course Examination

Course Examination

- 2 hours
- 50 questions to be answered with multiple choices
- Close-Book
  - NO for bringing PPTs and other readings
  - Paper Dictionary （English→ Chinese） is allowed

Another Sample:

Use the lightning network in a way that can ____ your payments

a. anonymize

b. complete

c. control

d. encrypt

Before the Exam

- **Read through the course materials**

  *.ppt, *.doc

- **Strategies:**

  Top-down, decomposition….

- **Think deeply**

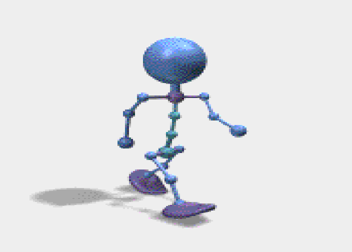
  Identify difference between the concepts

- **Sleep well**

  Don't stay over night prior to the exam !

- **Eat well**

  Don't skip the breakfast/lunch !



During the exam

-- Strategies for taking the exam

- **Read the questions carefully**

  Watch out for the words like “not”, “exclude” and “except”

- **Read all the answers**

  One technique is to read choice “D” first

- **Eliminate wrong choices**

  Cross out choices that look incorrect

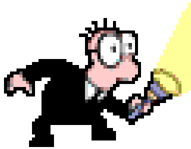
  If you’re still uncertain, circle the question and come back to it after you completed a first pass through the exam – don’t waste time.

- **Use “Common Sense” and “Logical Thinking”**

  There is NO magic puzzle

- **Choose the best answer**

  More than one answer may be technically correct



After the exam

- **Record the questions that is still confusing**

  Write up the question IDs and **key words**

- **Self validation**

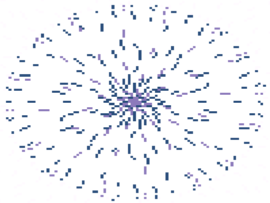
  Check the course materials using the **key words**

- **Mutual verification**

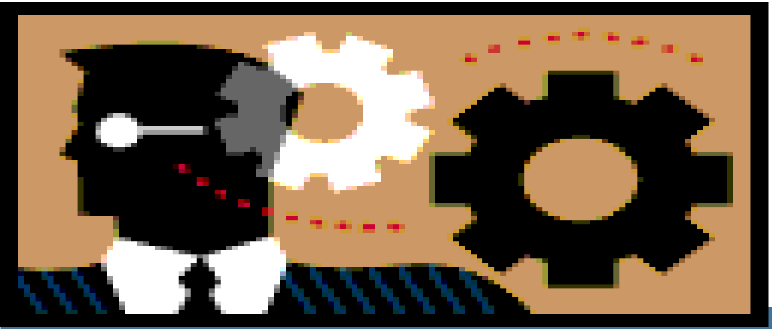
  Ask around for the right answers

- **Further Query**

  Send email to instructor with the question index number



Good Luck!



Lecture Outline

- ✓ Course Objectives
- ✓ A Day in Blockchain Utopia
- ✓ Bitcoin Development
- ✓ Smart Contracts
- ✓ Community, Politics, & Regulation
- ✓ The Fight for Privacy
- ✓ Scaling Bitcoin
- ✓ A Blockchain-Powered Future
- ✓ Course Examination

The END！

धन्यवाद

Hindi

Спасибо

Russian

شكرا

Arabic

Grazie

Italian

நன்றி

Tamil

多謝

Traditional Chinese

Thank You

English

多谢

Simplified Chinese

ありがとうございました

Japanese

ขอบคุณ

Thai

Gracias

Spanish

Obrigado

Brazilian Portuguese

Danke

German

Merci

French

감사합니다

Korean