Bitcoin, Blockchain Mini Workshop v 3.5

How this technology could impact your workplace & your career

empoweredlaw.com or @pamelawjd

About me

A. Created a niche career to fit my ideal lifestyle
B. Self-employed / Entrepreneur
    a. Educate lawyers
    b. Author
    c. Travel the world
    d. Only work with people I like on projects I like
C. I LOVE my work & my life

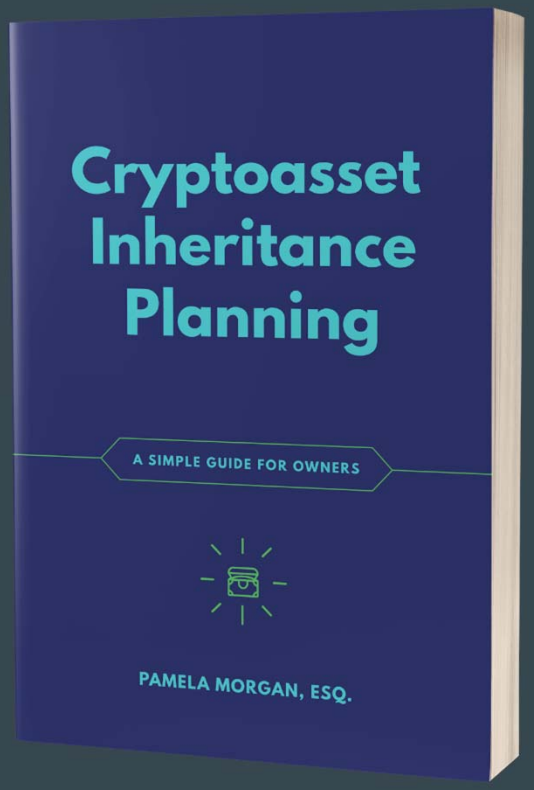
Work history: Westlaw, intern E.D. Mich, mid-size midwestern firm (summer), solo, in-house, franchise owner, professor, professional trainer, consultant, author

Third Key SOLUTIONS

EMPOWERED LAW

@pamelawjd

From a practical perspective, how will my loved ones access my cryptoassets when I'm not around to help them?



https://www.amazon.com/Cryptoasset-Inheritance-Planning-Simple-Owners/dp/1947910116/

@pamelawjd

Audience Poll

What kinds of projects exist today?

- Banking, Finance
- Escrow
- Tax
- Secured Transactions
- Real Property
- Estate Planning
- Government Policy
- Privacy Law
- Contracts
- ADR
- Insurance
- Non-Profit, NGO
- Intellectual Property
- International Law
- Equity Issuance
- Corporate Governance
- Funding & IPO
- Campaign Finance
- Central Bank Issuance
- Gaming
- Identity

CC BY SA

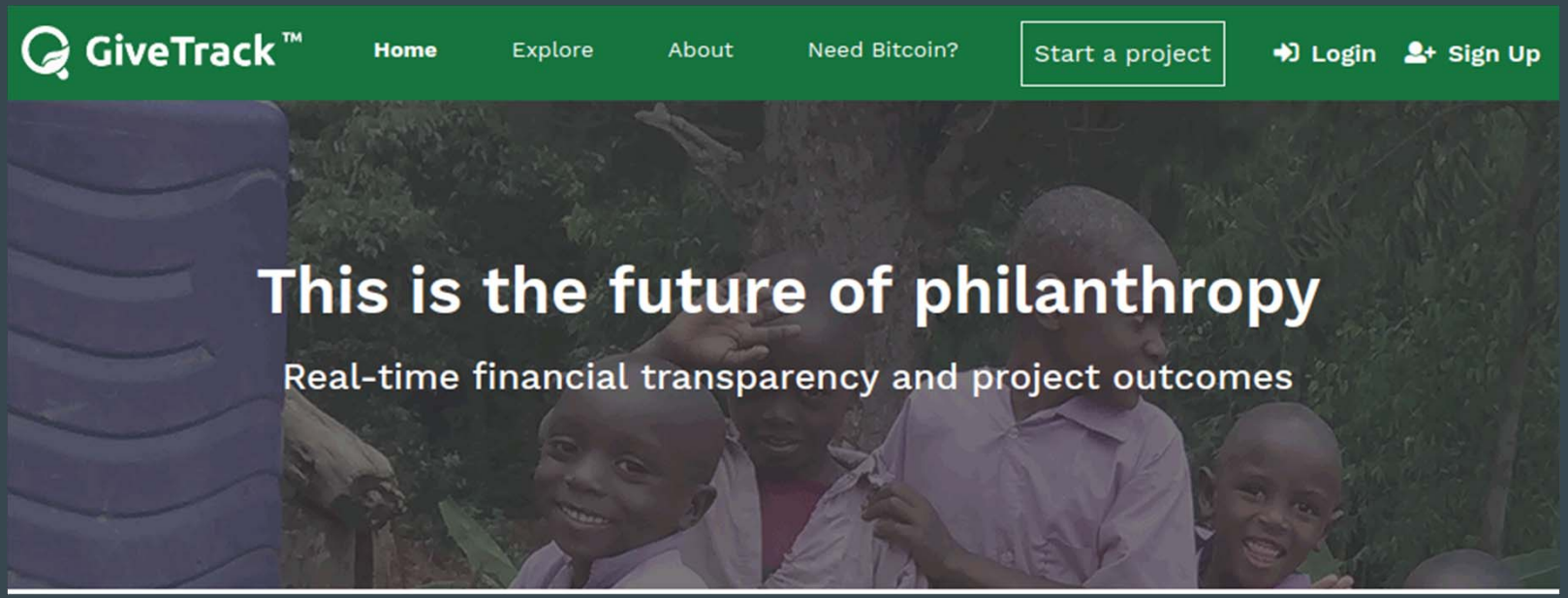
Novel Legal Issues

@pamelawjd

Paying Taxes with Bitcoin

@pamelawjd

GiveTrack



@pamelawjd

bitcoin

the currency

Bitcoin

the network

@pamelawjd

Bitcoin is an invention

https://bitcoin.org/bitcoin.pdf
Bitcoin is "The Internet of Money"

https://www.maxpixel.net/Pina-Colada-Cocktail-Alcohol-Drink-Recipe-Party-847246

Bitcoin is…

A. electronic, global peer-to-peer **cash**
B. an **invention** in computer science
C. a **trust** platform
D. a network **protocol**
E. an experiment
F. **all of the above**

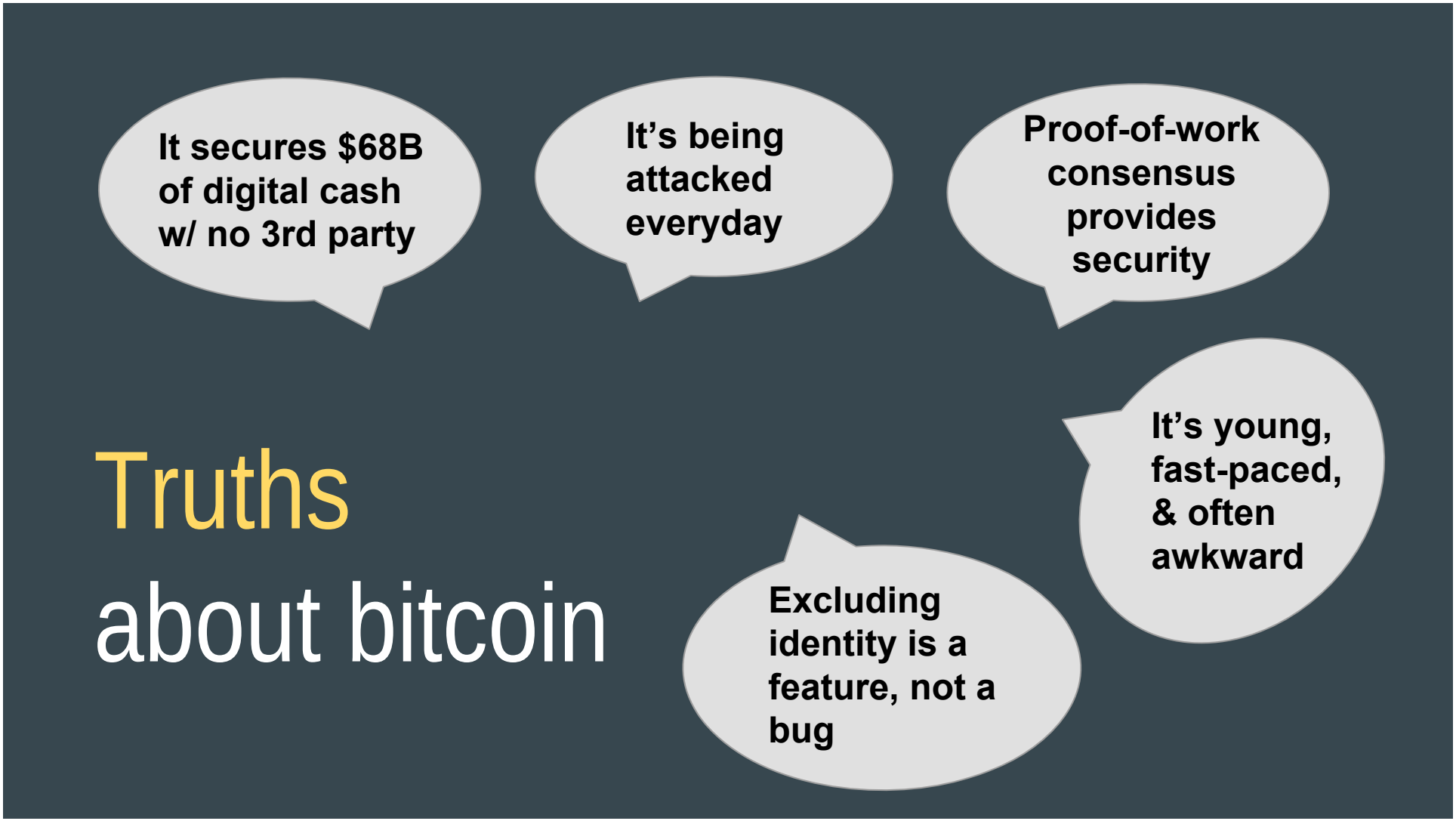
@pamelawjd

Terms of art:

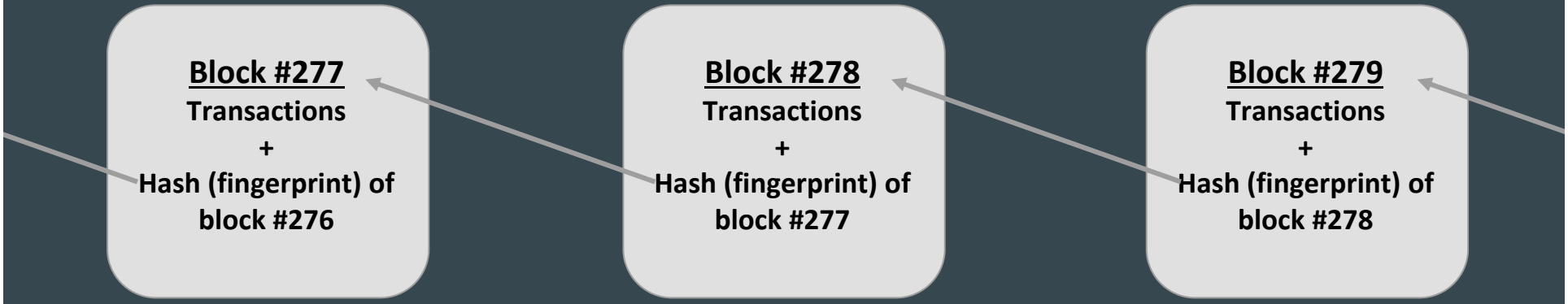
A. **a peer-to-peer network**: everyone is equal
B. **consensus rules**: what makes a transaction valid, what makes a block valid (future/present)
C. **validation**: testing against rules
D. **immutable:** ledger history more than a few days cannot be changed by anyone (PoW)
E. **proof-of-work**: uses an extrinsic asset to secure the network (unrecoupable costs)

@pamelawjd

It’s anonymous, it’s encrypted
Only drug dealers/bad people use it
It’s a pyramid scheme / not backed by anything
Mistaken beliefs about bitcoin
It is unregulated
It wastes energy

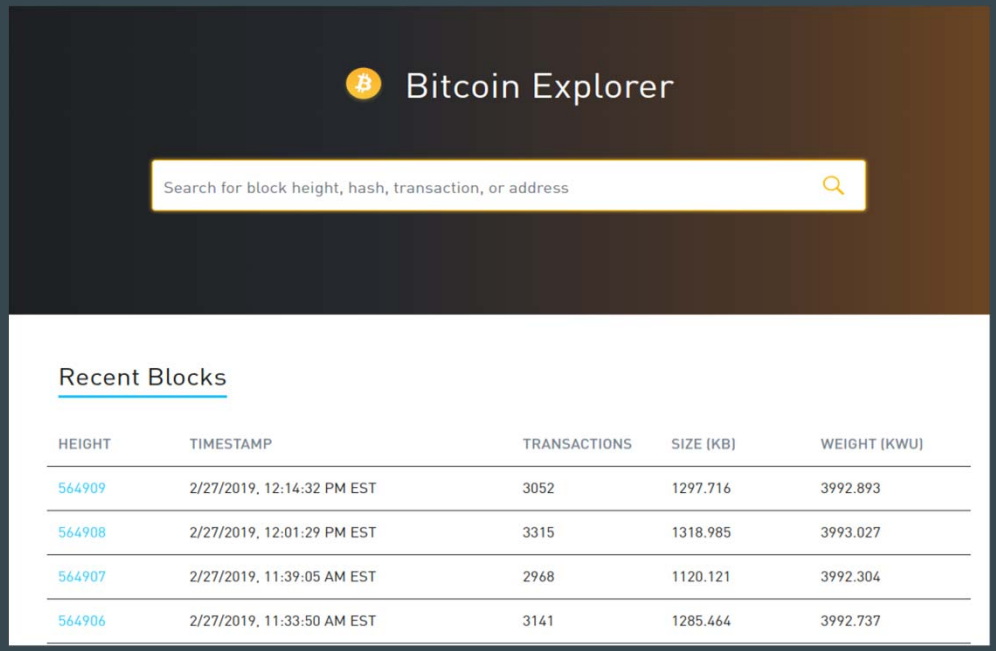

It secures $68B of digital cash w/ no 3rd party
It's being attacked everyday
Proof-of-work consensus provides security
It's young, fast-paced, & often awkward
Excluding identity is a feature, not a bug
Truths about bitcoin

What is a blockchain? A chain of blocks.



blocks of data, chained / linked together
with fingerprints (hashes)

Using Blockchain Explorers



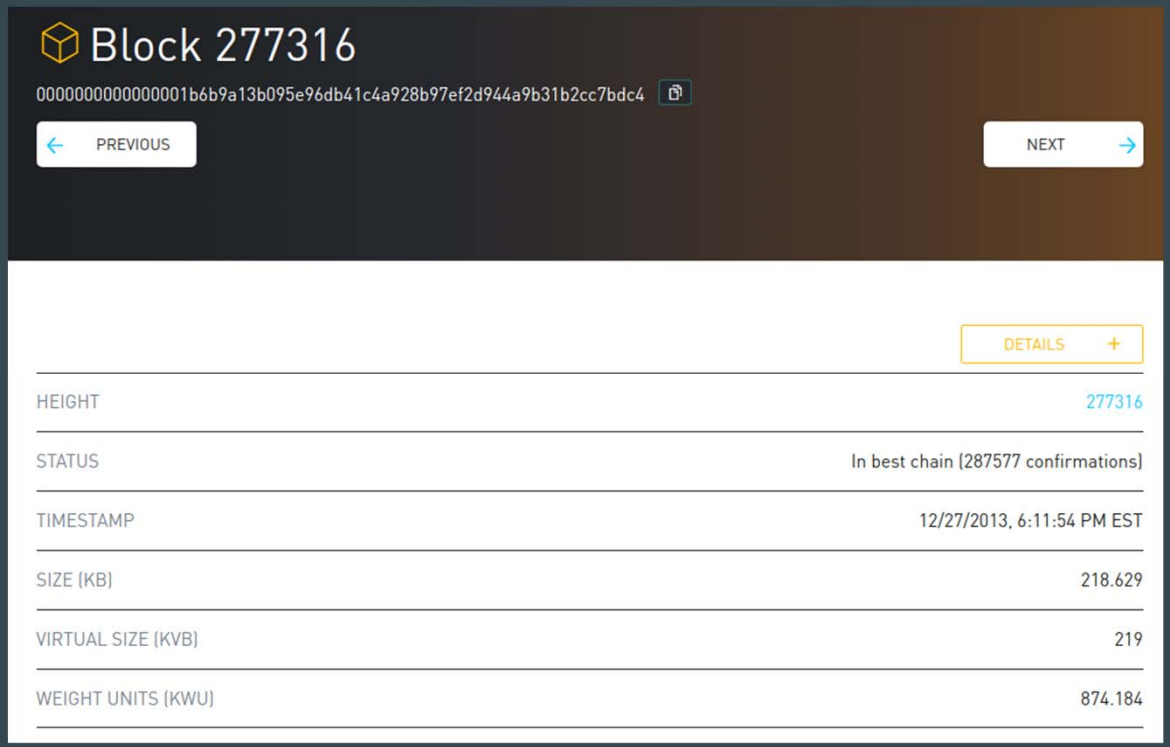
@pamelawjd

Go to blockstream.info

Look up block number 277316

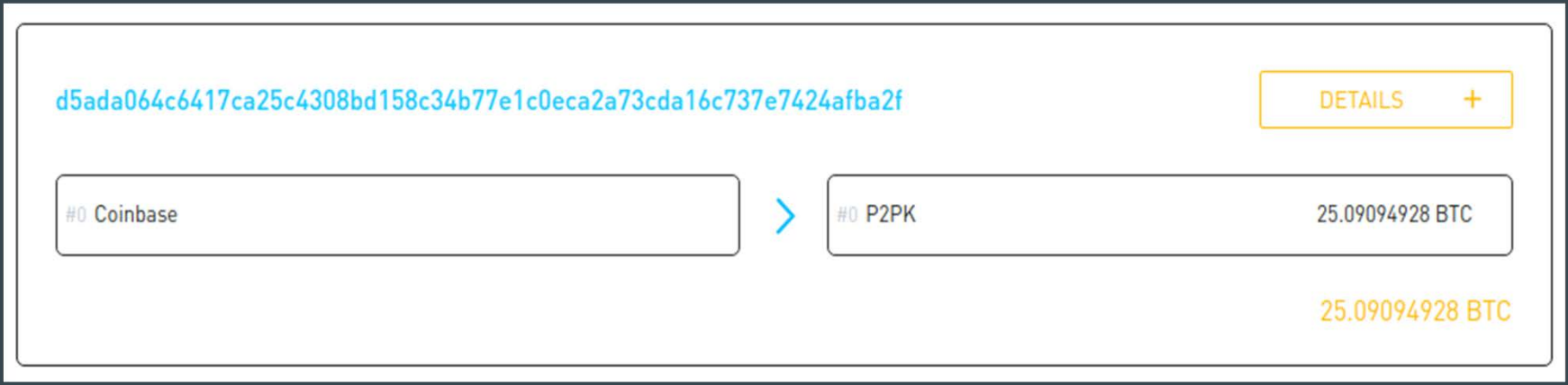
Mastering Bitcoin 2nd Edition at amazon.com or
https://github.com/bitcoinbook/bitcoinbook

Details for block 277316



@pamelawjd

Coinbase = Newly Minted Bitcoin



@pamelawjd

Use Example: Alice pays Bob for a cup of coffee

https://upload.wikimedia.org/wikipedia/commons/2/22/Mobile_payment_03.JPG

@pamelawjd

Alice Pays Bob

@pamelawjd

Find Alice's Payment to Bob

1. **Use the first 4 characters of Bob's Address to search for the transaction**

    a. **CTRL + f (find function in your browser)**
    b. **1Gdk (case sensitive)**

1. **Select Bob's Address to see the transaction history**

Bob’s Immortal Address

Address

1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA

CONFIRMED TX COUNT	32
CONFIRMED RECEIVED	32 outputs (0.26589525 BTC)
CONFIRMED UNSPENT	32 outputs (0.26589525 BTC)

@pamelawjd

Transactions to Bob

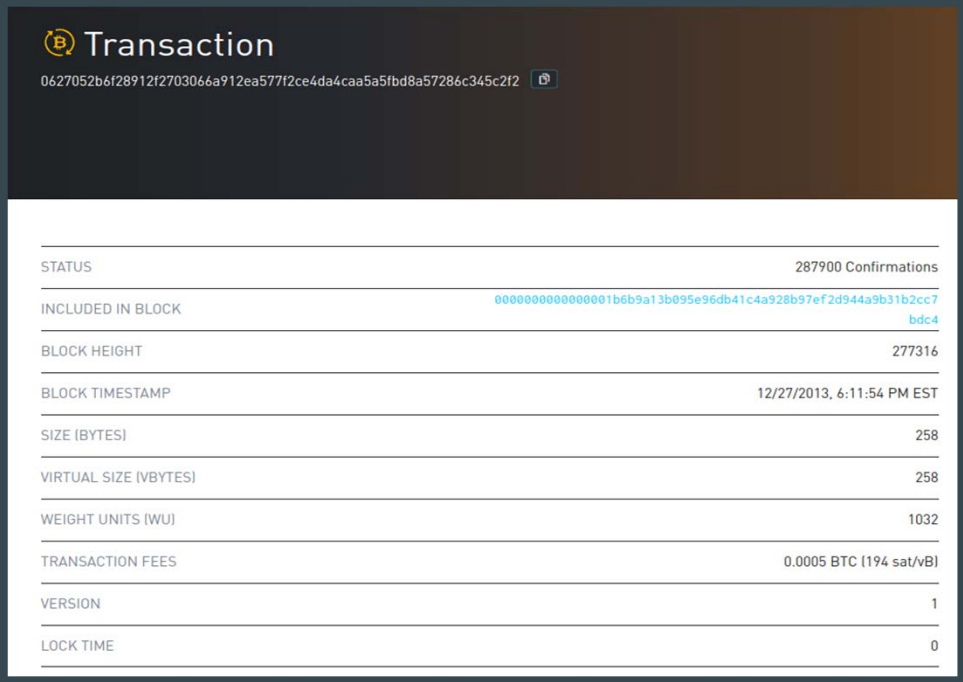
Typical tx:
1 input 2 output

Typical tx:
Change is first

Typical tx:
Aggregates inputs
Change is first

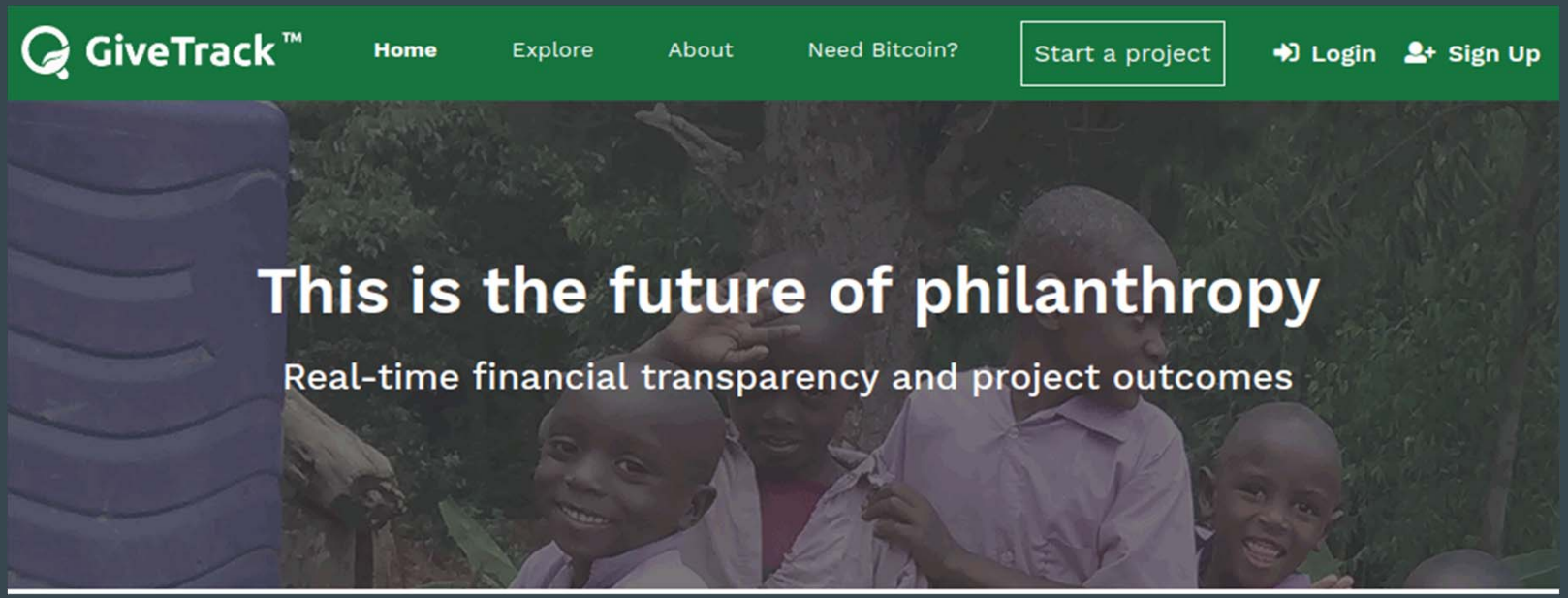
@pamelawjd

When was Bob's Address first funded?



@pamelawjd

GiveTrack.org: donation & audit transparency



Disclosure: I am an unpaid advisor to the BitGive Foundation

@pamelawjd

Questions?

Next up: blockchains, changing rules, & tokens

Bitcoin's blockchain

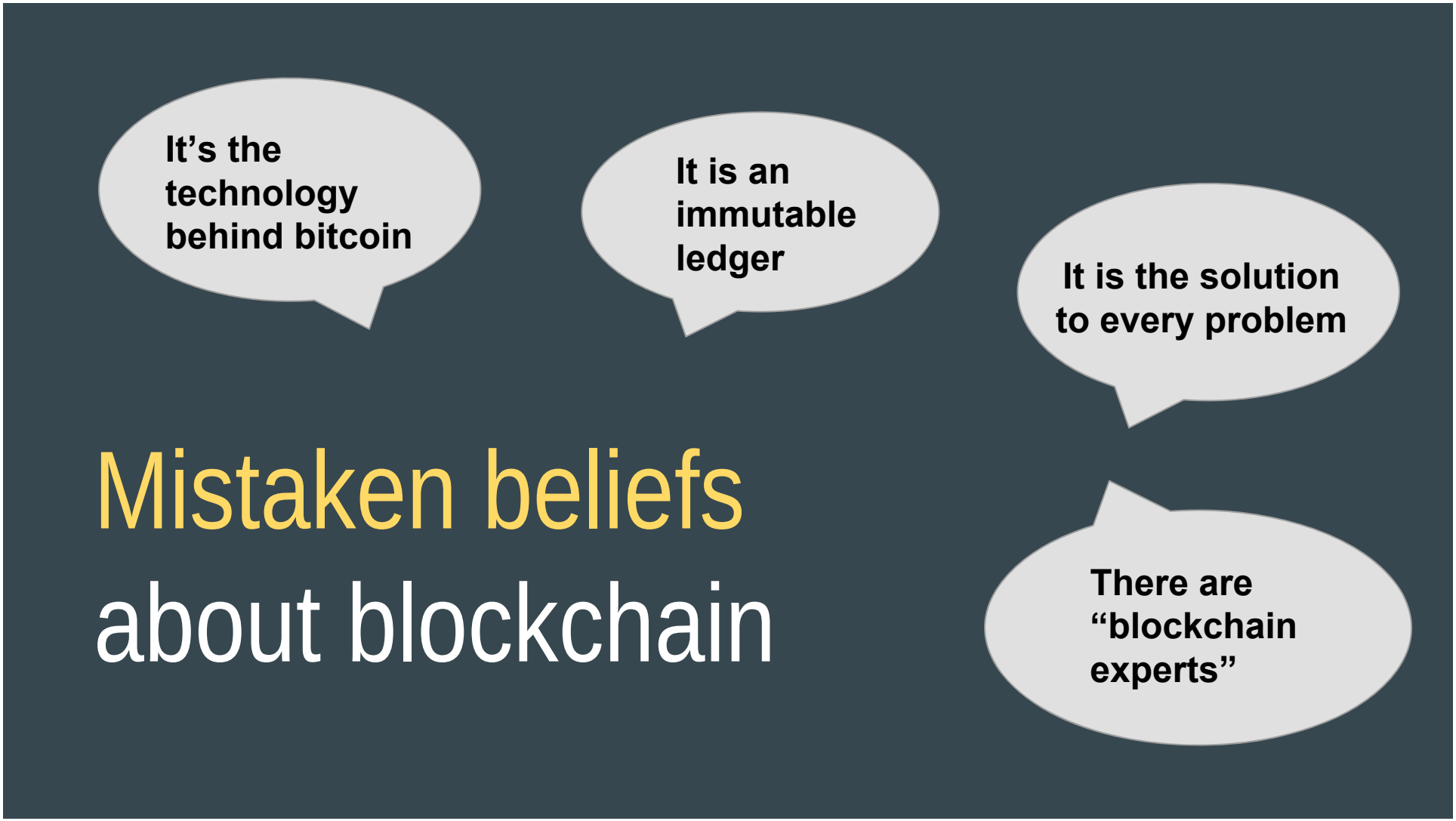
the immutable ledger where all bitcoin transactions are recorded and maintained

The Blockchain

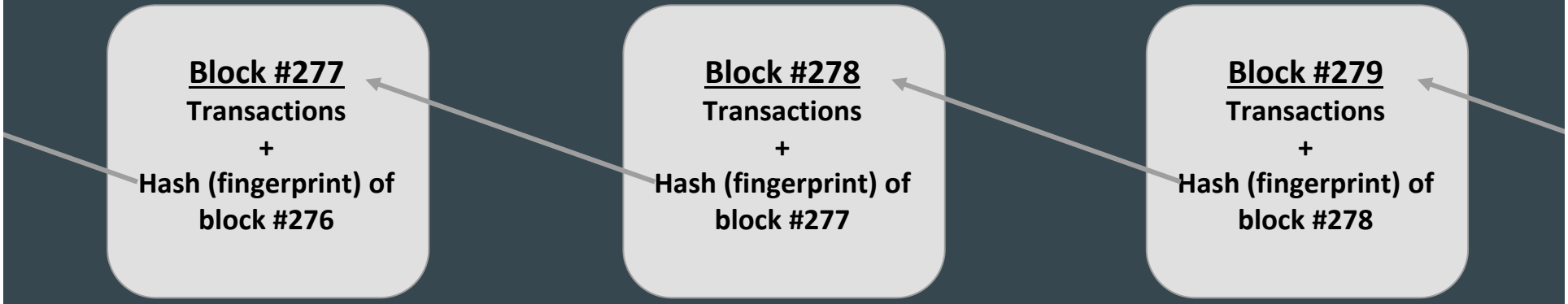
a meaningless term used by the confused or corrupt

see "blockchain will change everything"

@pamelawjd


It’s the technology behind bitcoin
It is an immutable ledger
It is the solution to every problem
Mistaken beliefs about blockchain
There are “blockchain experts”

What is a blockchain? A chain of blocks.



blocks of data, chained / linked together
with fingerprints (hashes)

The most important questions to ask about blockchain projects:

A. who can change the **future**

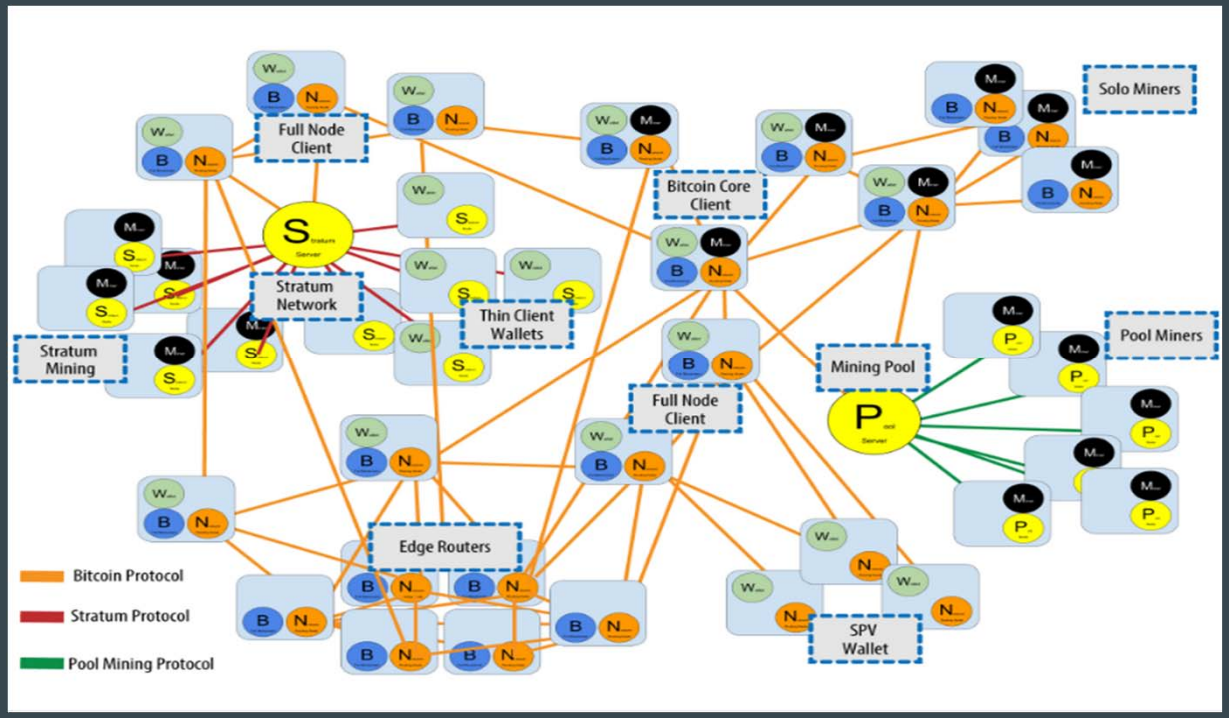
B. who can change the **past**

C. at what **cost**

D. **who will know, when, & how**

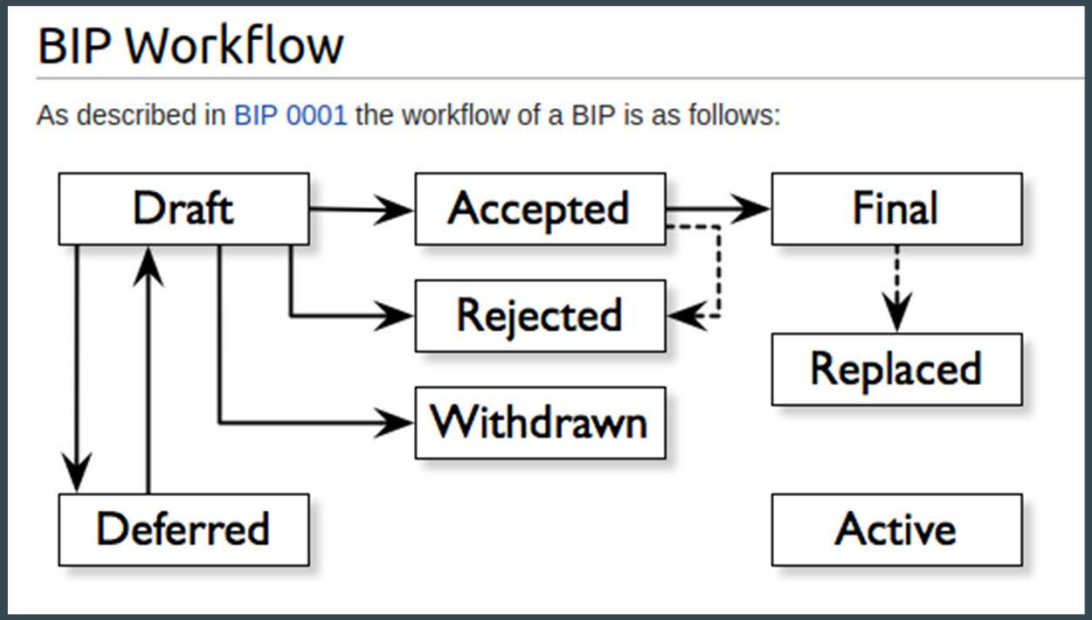
@pamelawjd

The Bitcoin Network



@pamelawjd

Changing the Future (upgrades)



https://en.bitcoin.it/wiki/Bitcoin_Improvement_Proposals
https://github.com/bitcoin/bips/blob/master/README.mediawiki

@pamelawjd

Changing the Past

Bitcoin Q&A: Energy consumption

https://www.youtube.com/watch?v=2T0OUIW89II&list=PLPQwGV1aLnTsHvzevl9BAUlfsfwFfU7aP&index=5

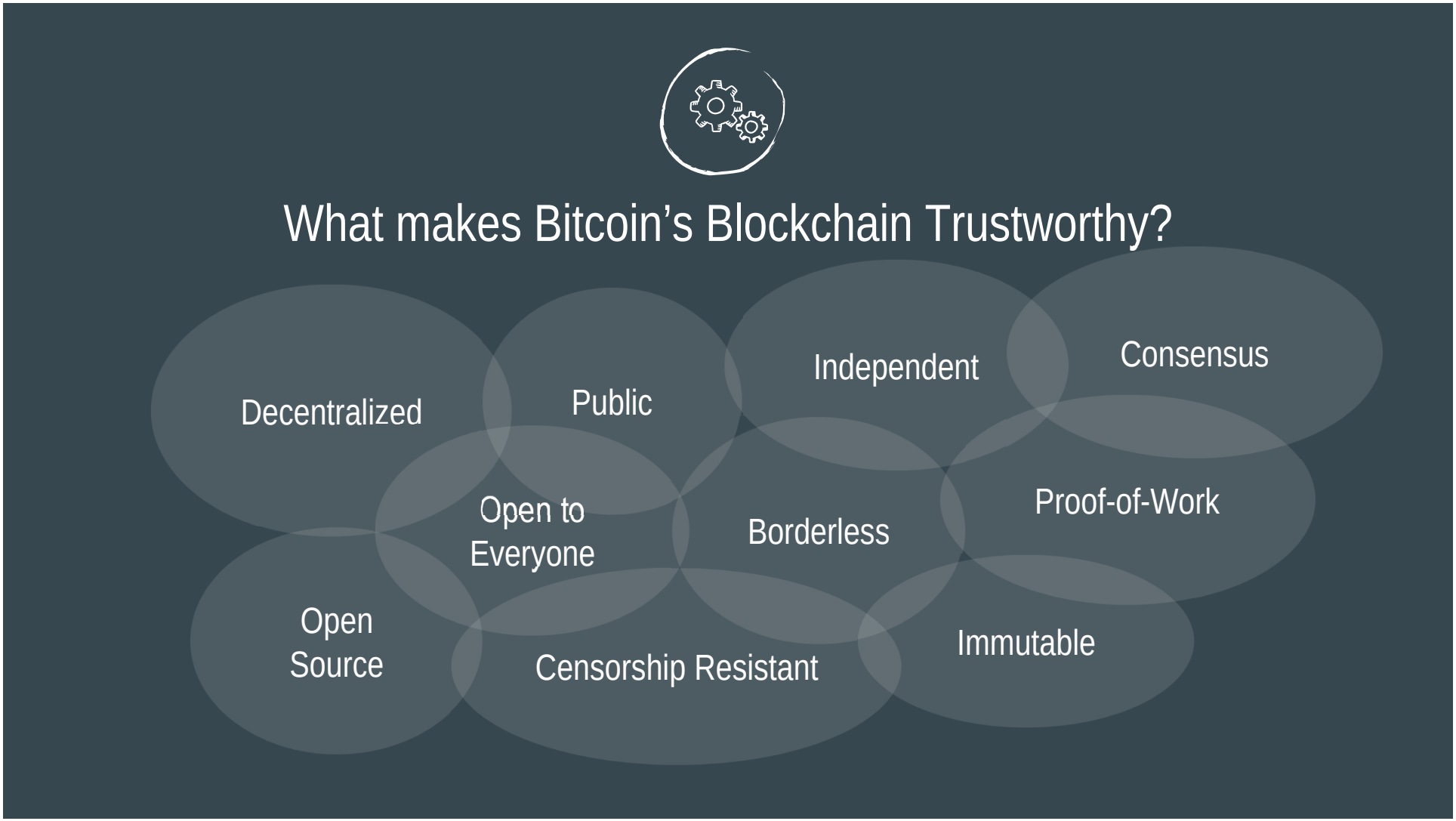
@pamelawjd

Who will know? When? How?

...

at what cost???

@pamelawjd


What makes Bitcoin’s Blockchain Trustworthy?
Decentralized
Public
Independent
Consensus
Open to Everyone
Borderless
Proof-of-Work
Open Source
Censorship Resistant
Immutable

The DAO Case Study

https://www.smithandcrown.com/sale/thedao/

@pamelawjd

ethereum.org

Build unstoppable applications

Ethereum is a **decentralized platform that runs smart contracts**: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference.

These apps run on a custom built **blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property.**

This enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middleman or counterparty risk.

The project was bootstrapped via an ether presale in August 2014 by fans all around the world. It is developed by the Ethereum Foundation, a Swiss non-profit, with contributions from great minds across the globe.

On traditional server architectures, every application has to set up its own servers that run their own code in isolated silos, making sharing of data hard. If a single app is compromised or goes offline, many users and other apps are affected.

On a blockchain, anyone can set up a node that replicates the necessary data for all nodes to reach an agreement and be compensated by users and app developers. This allows user data to remain private and apps to be decentralized like the Internet was supposed to work.

@pamelawjd

The DAO promises

A. The DAO, a distributed autonomous organization is holding an ICO. It is not quite a crowdsale: the DAO is selling ownership of itself and raising ETH in the process. The DAO's first act will be to hire Slock.it to do their work.

A. The tokens represent ownership over the DAO, which includes being able to nominate and vote on DAO activities, nominate and vote on DAO curators. At any point, token holders can burn their tokens and retrieve their unspent ETH.

A. Any profits the DAO makes on its investments will be given back to token holders as dividends.

@pamelawjd

The Attack

A. A rightful DAO token holder found a way to use the “get out of this investment” part of the smart contract to direct ETH to a new wallet controlled by the token holder. But not just their funds....

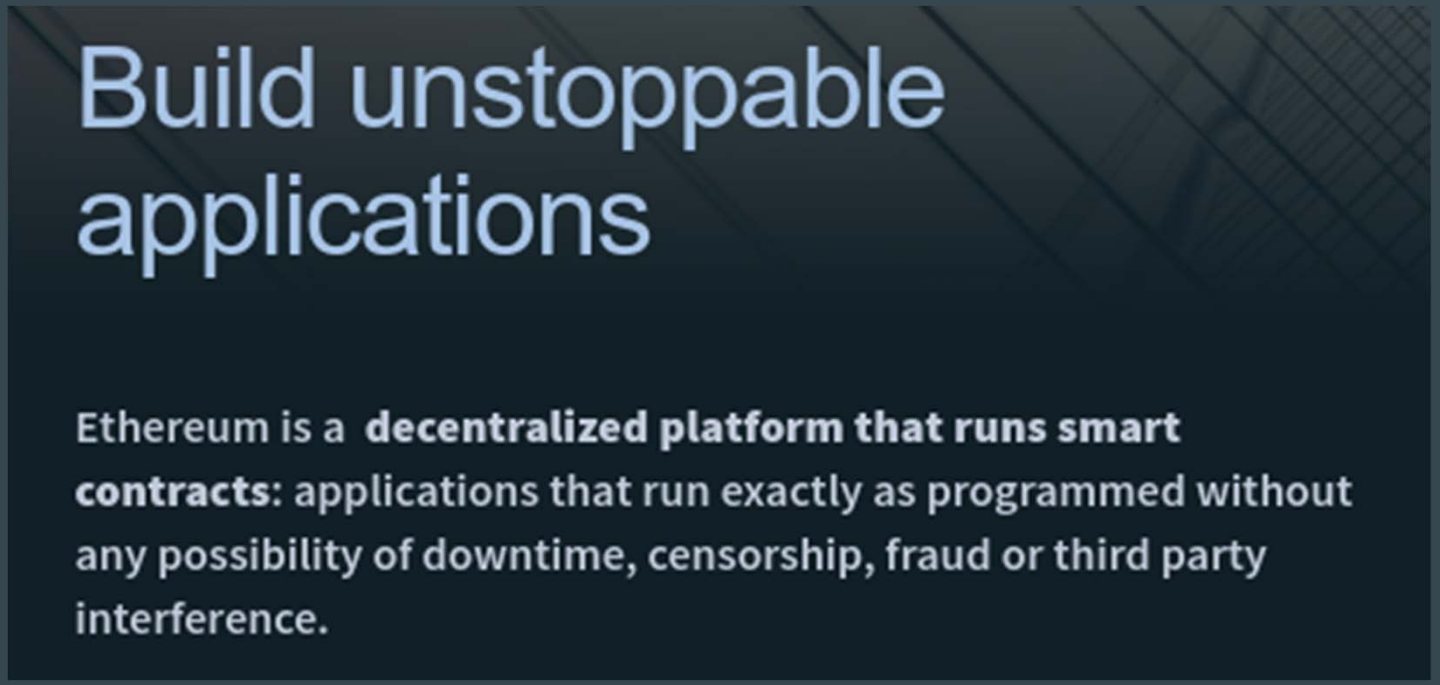
A. The community watched, in horror, as ETH streamed out of the DAO and into a private account. $150m became $125m became $90m...

@pamelawjd

ETH Price During the Attack

@pamelawjd

Ethereum Promises



@pamelawjd

Small Group Discussion: assume someone can intervene.

What, if a

@pamelawjd

Two Perspectives - - Who is Right?

We must intervene:
Theft is Wrong
Justice Required

Proof-of-Stake

We can't intervene:
Known Risks
Sets Precedent
Breaks Immutability
Code is law

@pamelawjd

Proposal: Freeze & Refund

...

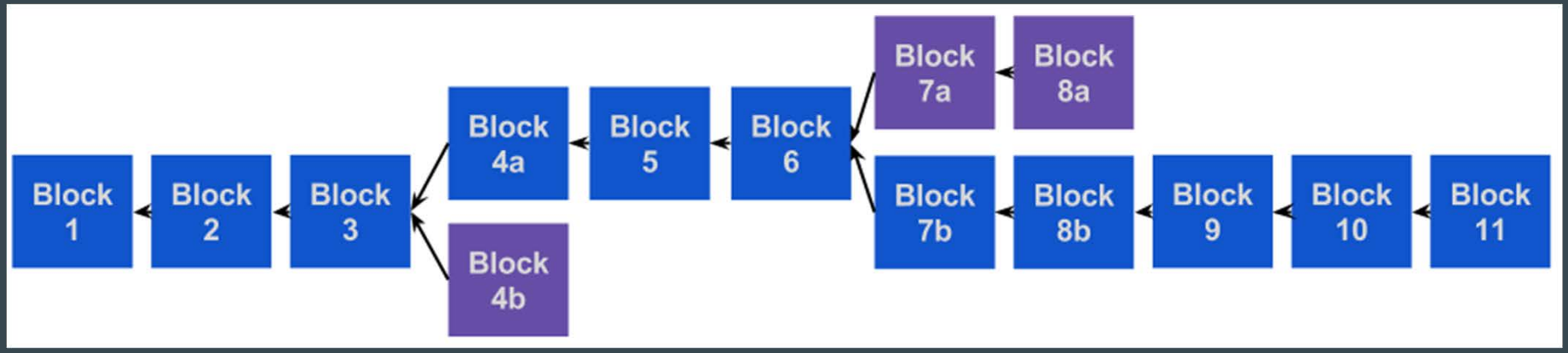
Freeze The DAO code base smart contract (all instances)
Change consensus rule to RefundDAO code
(effectively the first smart contract bankruptcy)

@pamelawjd

Meet ETH & ETC - Different Consensus Rules

@pamelawjd

What is a network fork?



Hard Fork v Soft Fork, Contentious v Not, Accidental v Intentional

Forkology by Andreas M. Antonopoulos

@pamelawjd

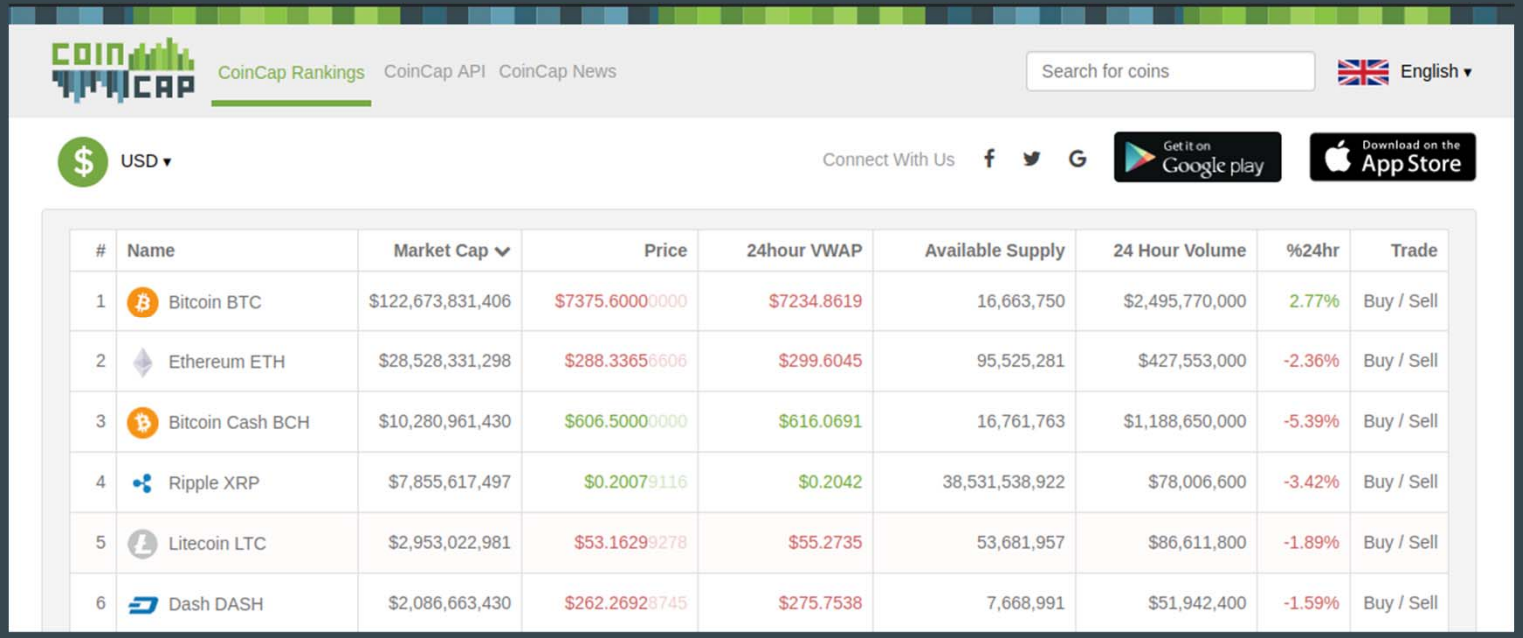
Questions?

Next up: so many tokens

Not Just Bitcoin….

Let’s look at other tokens (and learn how you can create your own)

How Many Tokens?



#	Name	Market Cap	Price	24hour VWAP	Available Supply	24 Hour Volume	%24hr	Trade
1	Bitcoin BTC	$122,673,831,406	$7375.60000000	$7234.8619	16,663,750	$2,495,770,000	2.77%	Buy / Sell
2	Ethereum ETH	$28,528,331,298	$288.33656606	$299.6045	95,525,281	$427,553,000	-2.36%	Buy / Sell
3	Bitcoin Cash BCH	$10,280,961,430	$606.50000000	$616.0691	16,761,763	$1,188,650,000	-5.39%	Buy / Sell
4	Ripple XRP	$7,855,617,497	$0.20079116	$0.2042	38,531,538,922	$78,006,600	-3.42%	Buy / Sell
5	Litecoin LTC	$2,953,022,981	$53.16299278	$55.2735	53,681,957	$86,611,800	-1.89%	Buy / Sell
6	Dash DASH	$2,086,663,430	$262.26928745	$275.7538	7,668,991	$51,942,400	-1.59%	Buy / Sell

@pamelawjd

ethereum.org

@pamelawjd

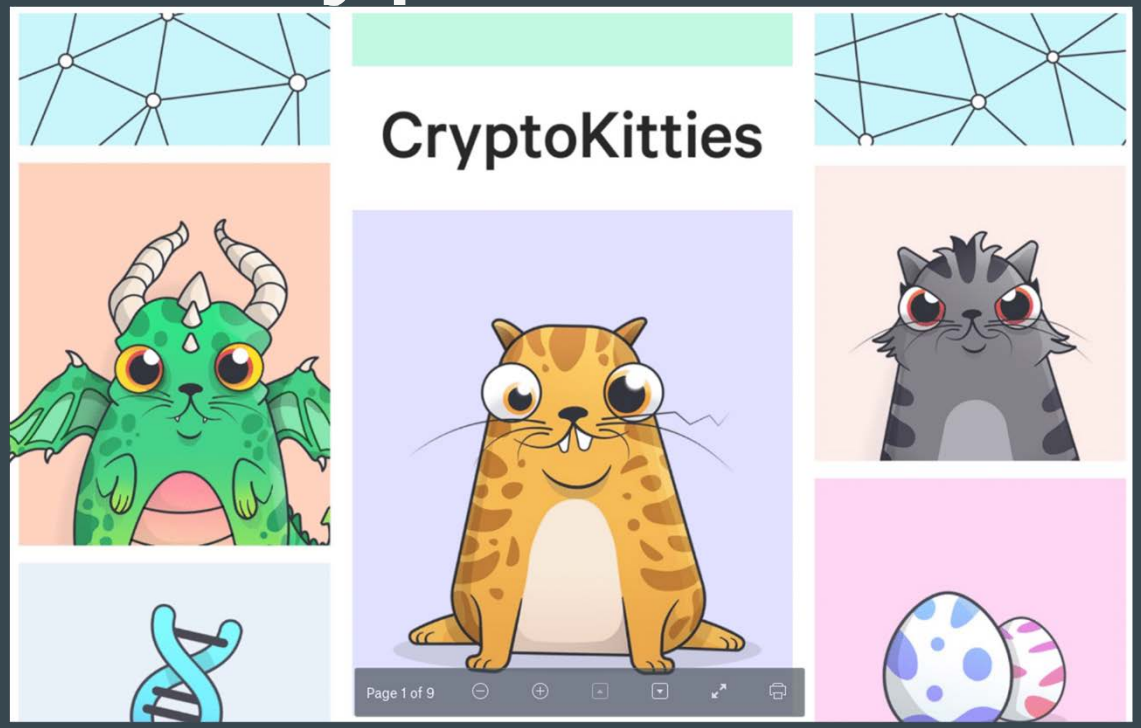
Bjork's Reportedly Giving Away Cryptocurrency With Her New Album

Rhett Jones
Yesterday 3:48pm • Filed to: CRYPTOCURRENCY 20 2

Photo: Associated Press

@pamelawjd

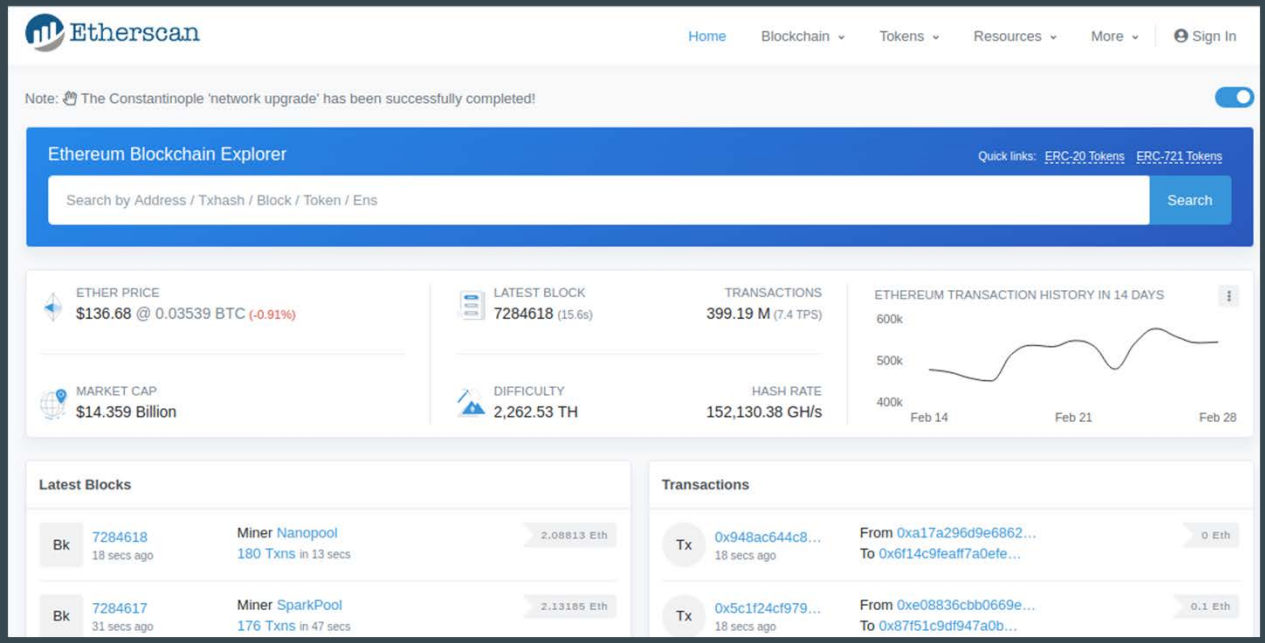
Crypto Kitties



@pamelawjd

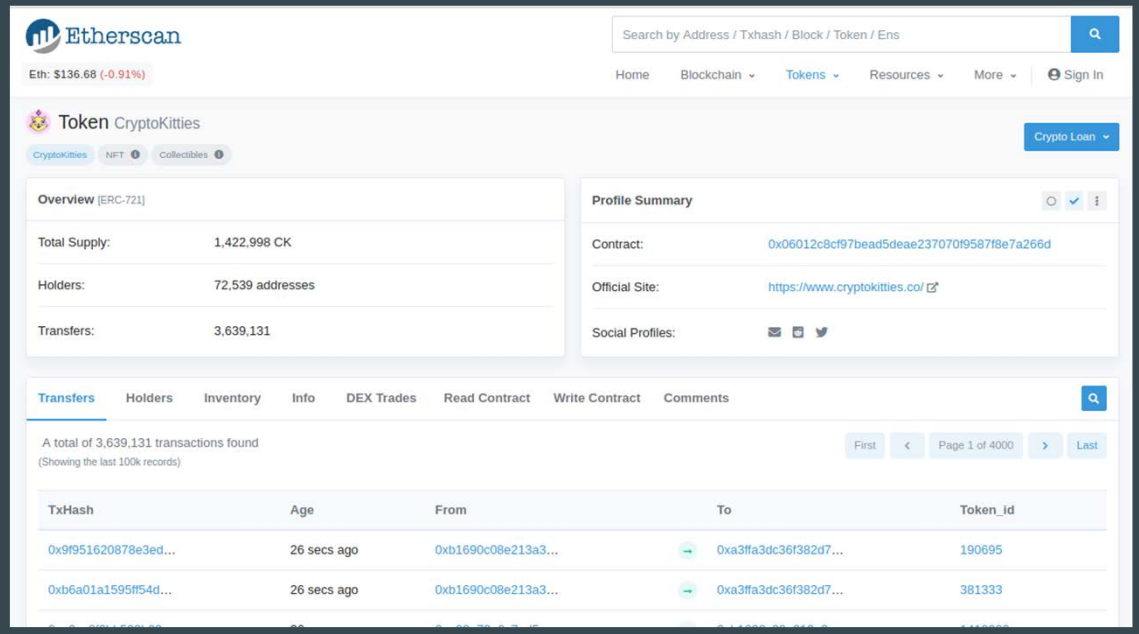
https://ethfiddle.com/09YbyJRfiI

Etherscan.io - Ethereum Blockchain Explorer



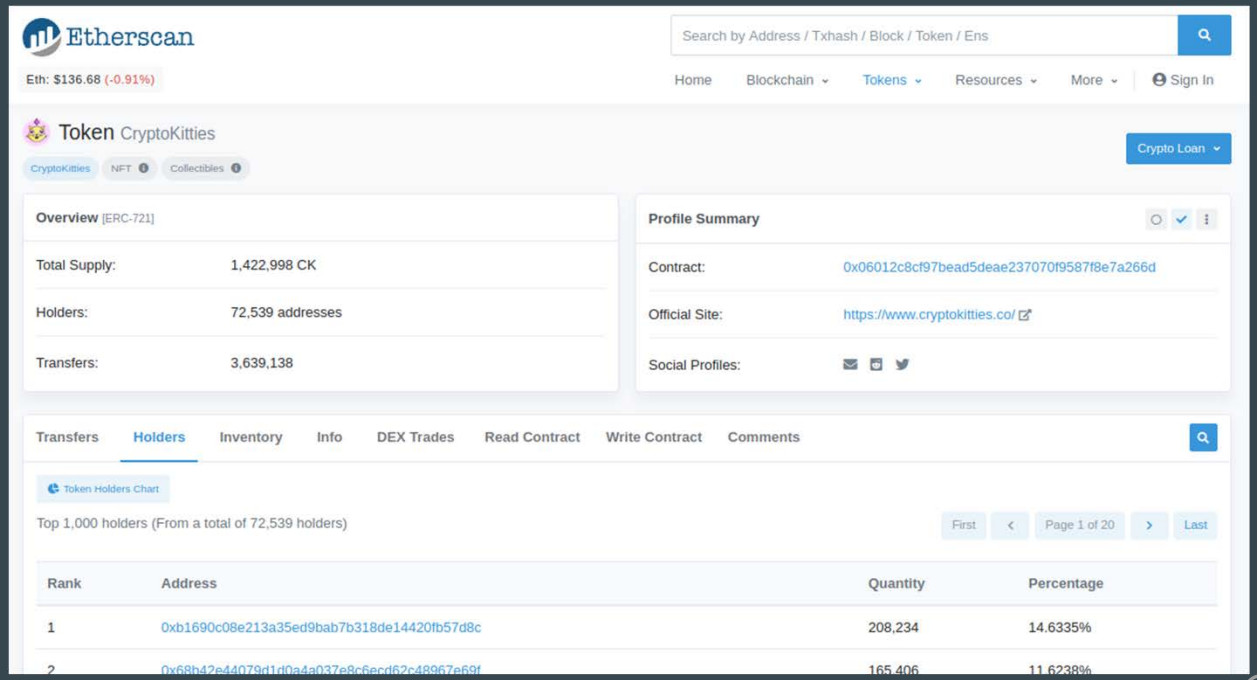
@pamelawjd

Search for CryptoKitties Token



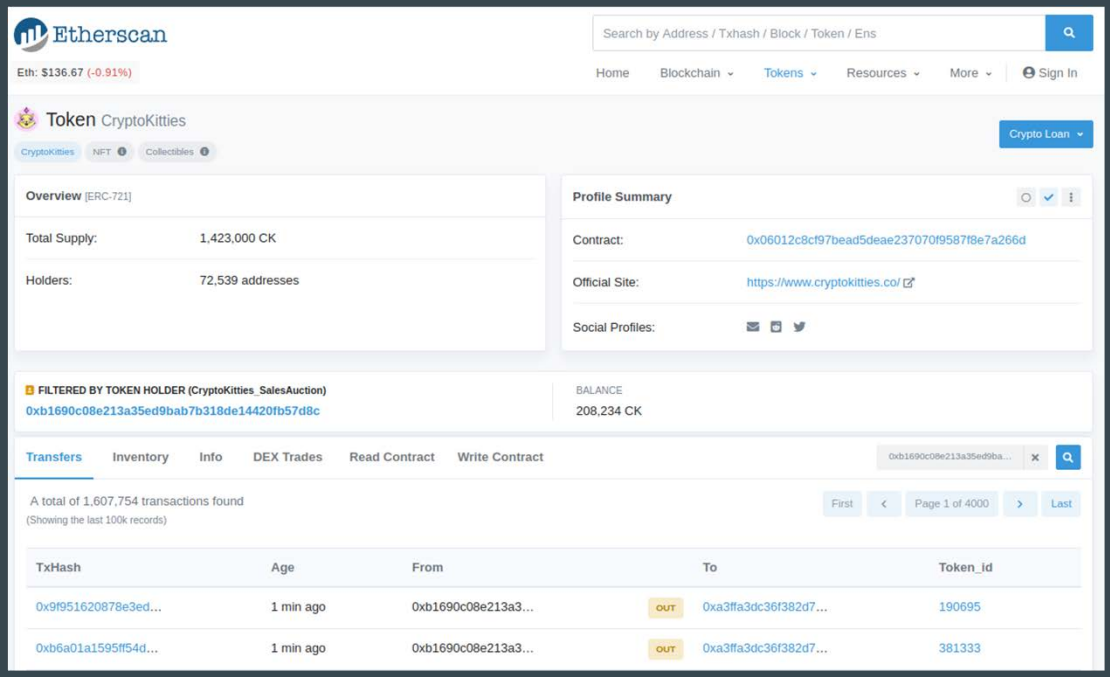
@pamelawjd

Find Who Owns the Most CryptoKitties Tokens



@pamelawjd

Look at their transaction history



@pamelawjd

Questions?

Next up: case study, taxes, and use cases

Paying Taxes with Bitcoin

@pamelawjd

Taxes in the U.S.

A. IRS Guidance: virtual currencies are property
B. Must Read: https://coincenter.org/pdf/BitcoinTaxesCalvin.pdf
C. Libra Tax Software

@pamelawjd

Accepting Cryptocurrencies for Payment

A. **Download and backup a wallet**
B. **Price earned income in your local currency**
C. **Specify source for exchange rate (e.g. CME, BRR)**
D. **Accept payment in 3 minutes or less**
E. **Immediately convert or set cost basis**

@pamelawjd

How to get bitcoin or other cryptocurrency

A. Download a wallet application (e.g. Blue, Jaxx)

A. Buy it: exchanges, bitcoin ATM, a friend
B. Earn it: accept it for payment of services
C. Gift: ask for it

@pamelawjd

Vital Record: Key Backup

Without a key backup, you could lose access forever
With the backup, full access; anywhere anytime
No third parties to compel

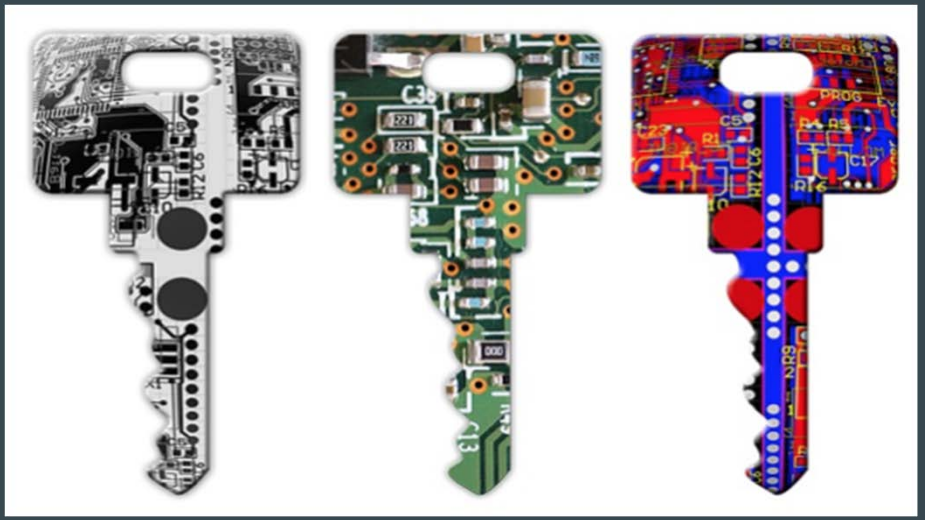
Use Cases

Features of Bitcoin & some other open public blockchains that can solve real problems for real people

Escrow without Custody

Superior client trust account:

multisig BTC



@pamelawjd

Get Your Security Deposit Back

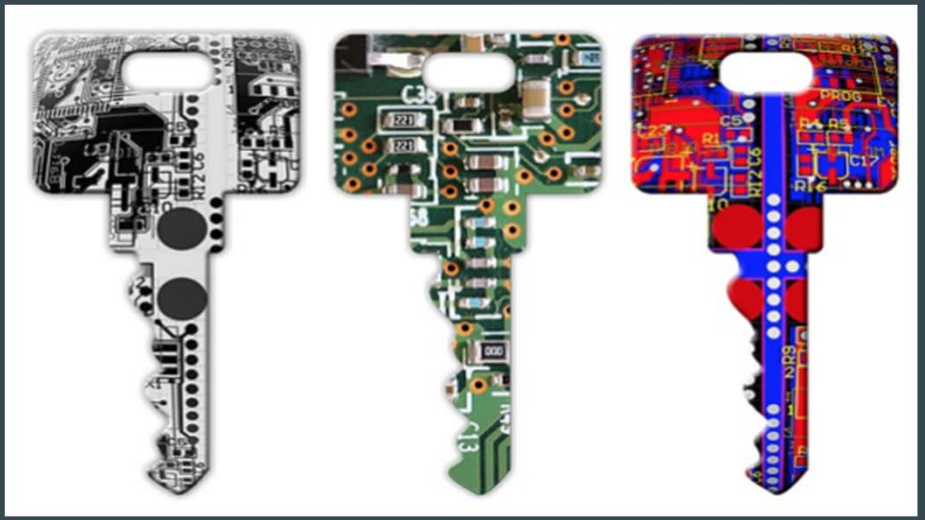
Balancing the power between landlords and tenants using multisig

@pamelawjd

Dispute Resolution

ADR Friendly

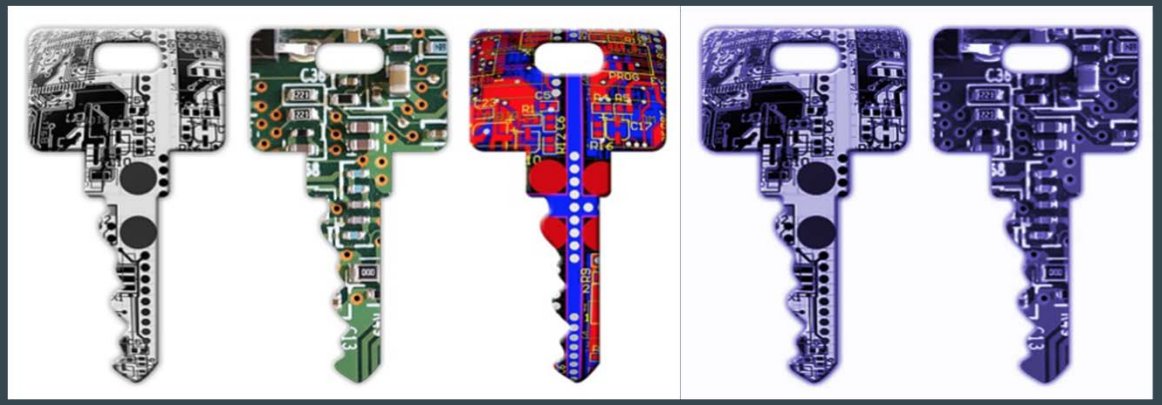
AAA Commercial Arbitrator



@pamelawjd

Governance & Audits

Investors can see everything in real time, no auditor report required

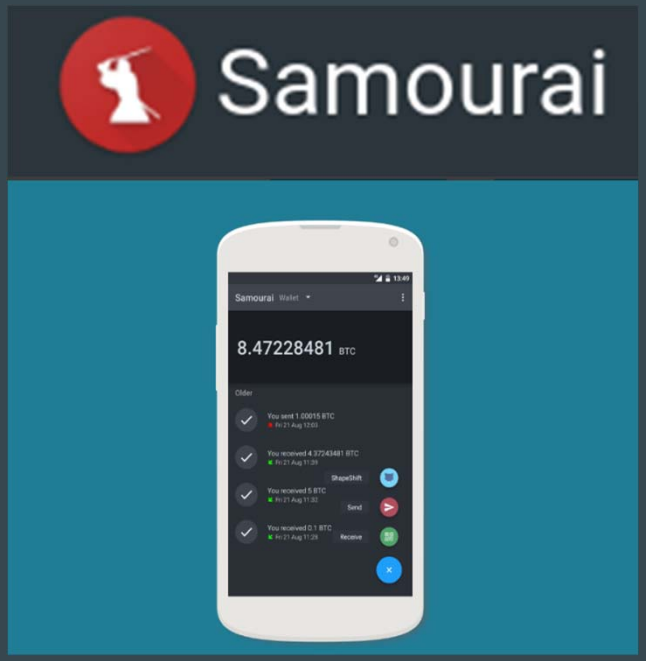


@pamelawjd

Empowering the Powerless

Hidden Wallet &
Privacy Features:

saving $ to escape
abuse, unsafe places



@pamelawjd

Streaming Money & Micropayments

Turning revenue streams into cash flow

Paying for attention

https://unsplash.com/photos/4z_SYrG5mgA

@pamelawjd

Crypto Currency Security Standard (CCSS)

CRYPTOCURRENCY SECURITY STANDARD	LEVEL I	LEVEL II	LEVEL III
Key/Seed Generation	✔		
Wallet Creation	✔	✔	✔
Key Storage	✔		
Key Usage	✔	✔	
Key Compromise Policy	✔	✔	
Keyholder Grant/Revoke Policies & Procedures	✔	✔	✔
Third-Party Security Audits/Pentests	✔		
Data Sanitization Policy	✔	✔	✔
Proof of Reserve	✔		
Audit Logs	✔	✔	

@pamelawjd

Flaw crippling millions of crypto keys is worse than first disclosed

Estonia abruptly suspends digital ID cards as crypto attacks get easier and cheaper.

DAN GOODIN - NOV 6, 2017 10:10 PM UTC

Enlarge / A digital identity card issued by the Republic of Estonia.

@pamelawjd

Security Bug - $200m +

Security Alert

7 November 2017

Severity: Critical

Product affected: Parity Wallet (multi-sig wallets)

Summary: A vulnerability in the Parity Wallet library contract of the standard multi-sig contract has been found.

Affected users: Users with assets in a multi-sig wallet created in Parity Wallet that was deployed after 20th July.

@pamelawjd

EMPOWERED **LAW**

Free Resources

For owners & professionals

Empoweredlaw.com

sign up for our newsletter

CC BY SA

Questions?

Thank You!

...

Contact: **pamela@empoweredlaw.com**

@pamelawjd