TECHNISCHE UNIVERSITÄT WIEN
Vienna | Austria

Christian Doppler Forschungsgesellschaft

SBA Research

COMET
Competence Centers for Excellent Technologies

Blockchain: You’re Doing it Wrong

bmvit Bundesministerium für Verkehr, Innovation und Technologie

bmwfw Bundesministerium für Wissenschaft, Forschung und Wirtschaft

FFG

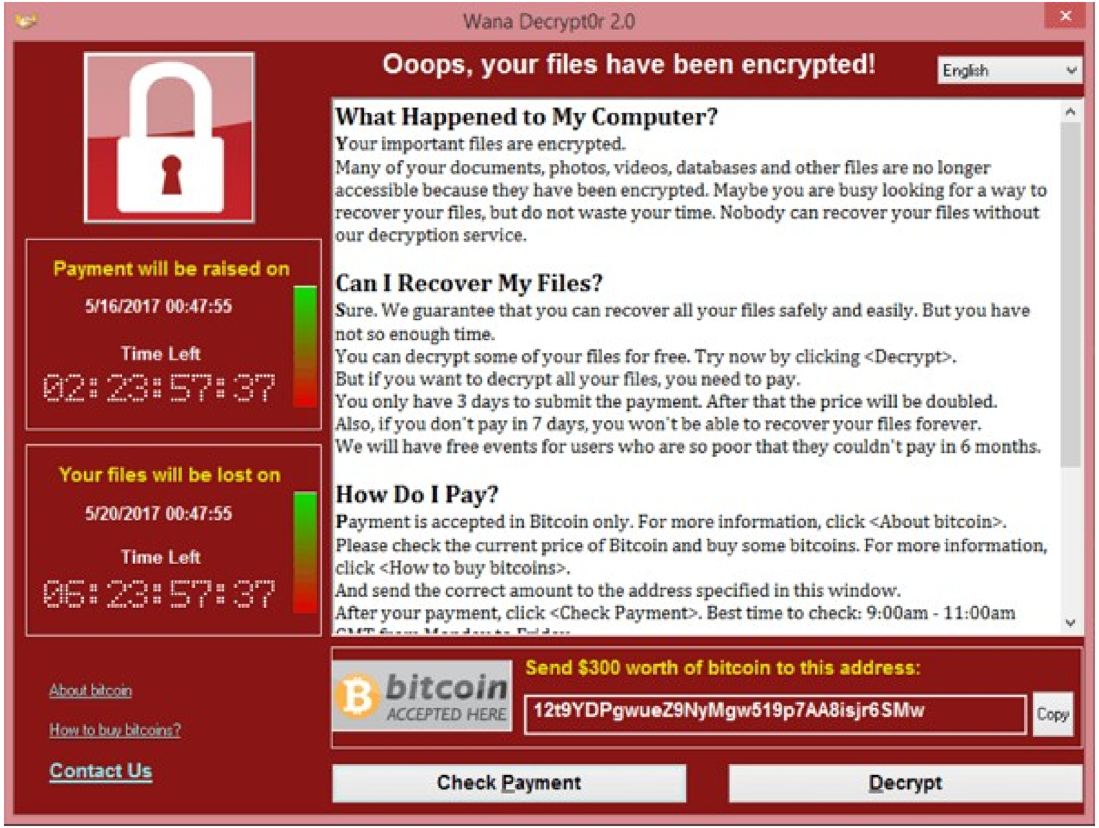
wirtschafts agentur wien
Ein Fonds der Stadt Wien

FWF

Christian Doppler Forschungsgesellschaft

netidee powerful innovations

Blockchain Technologies will negatively affect YOU!



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

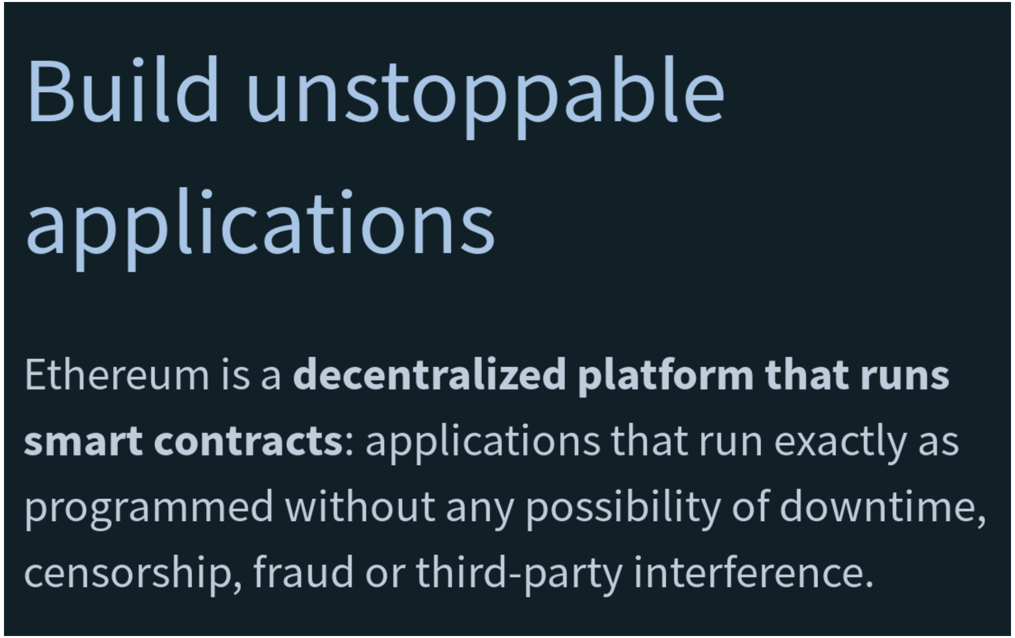
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Source: https://commons.wikimedia.org/wiki/File:Wana_Decrypt0r_screenshot.png

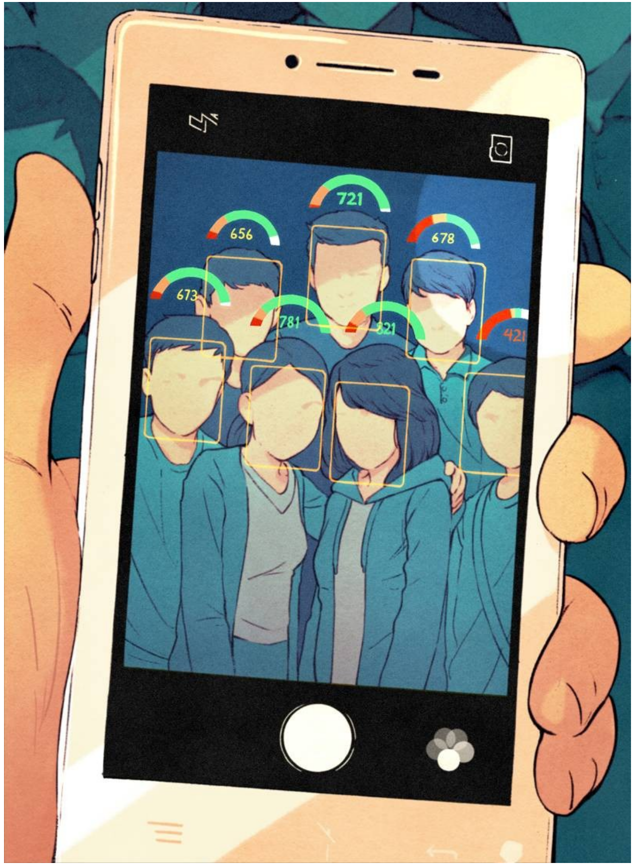
Interesting Read: "The ring of Gyges: Investigating the future of criminal smart contracts.", Juels et al., ACM SIGSAC 2016



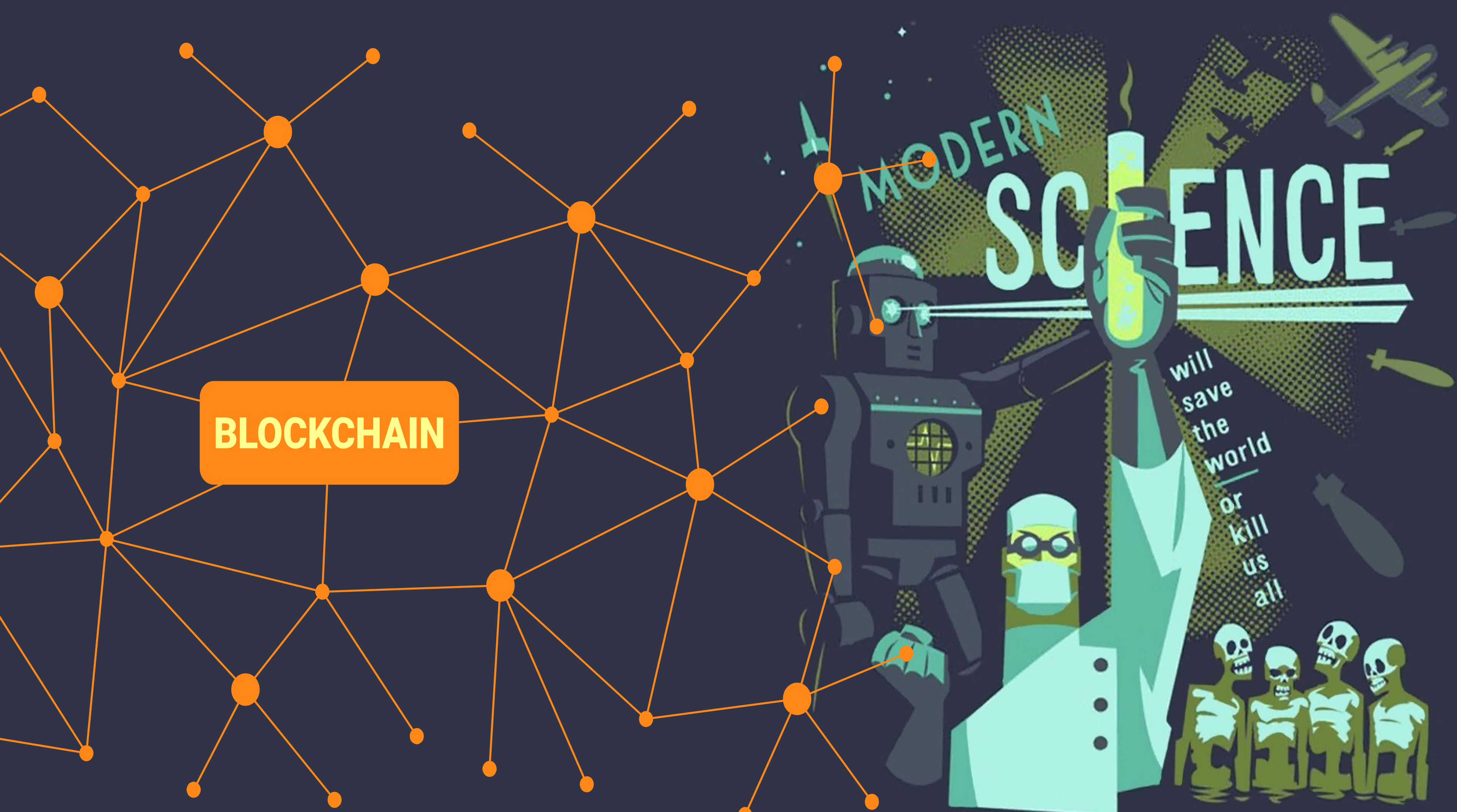
Build unstoppable applications

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.

Source: https://www.ethereum.org/



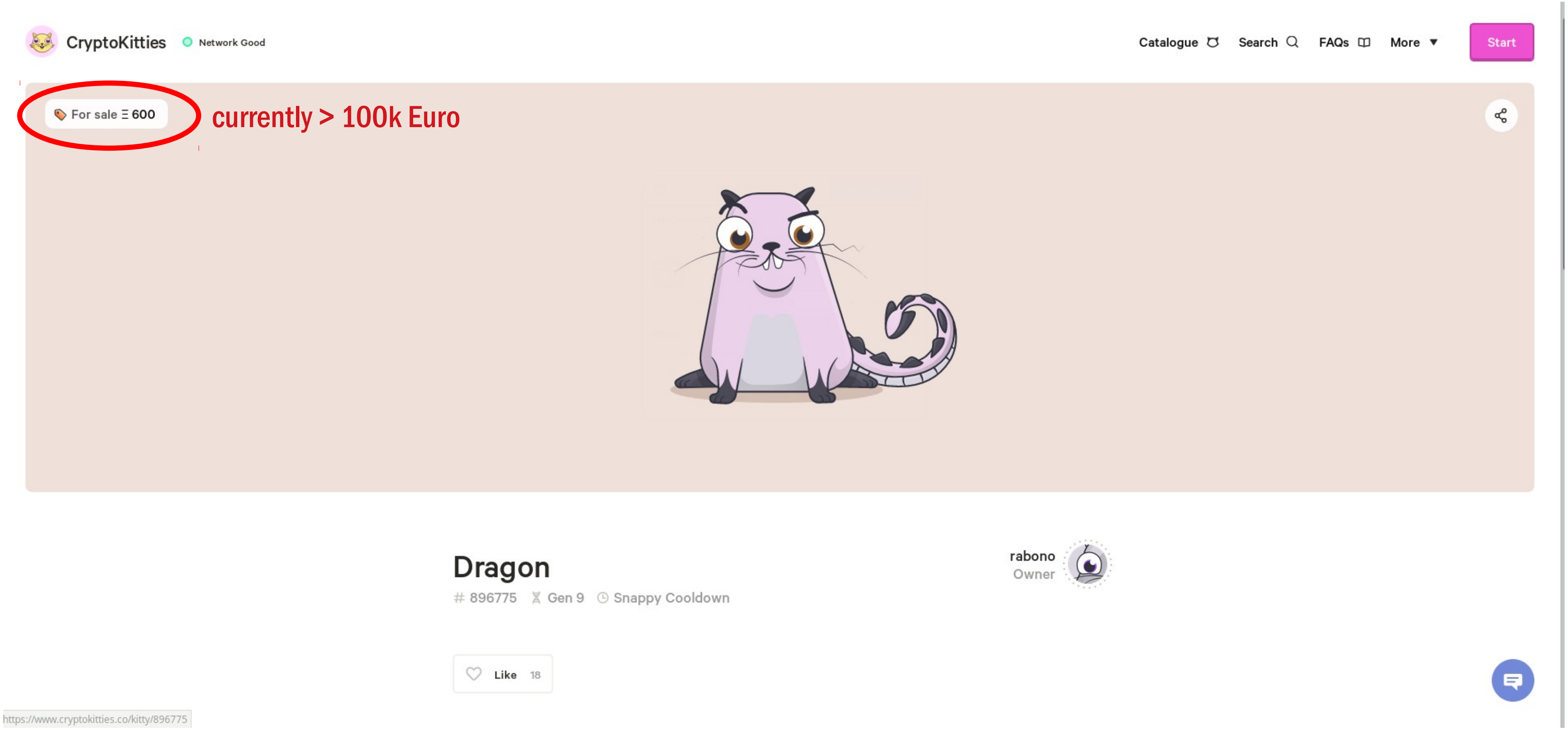
Kevin Hong,
https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion



BLOCKCHAIN

Source: https://www.wallpapervortex.com/

Blockchain: Fear of Missing Out



For sale Ξ 600

currently > 100k Euro

Dragon

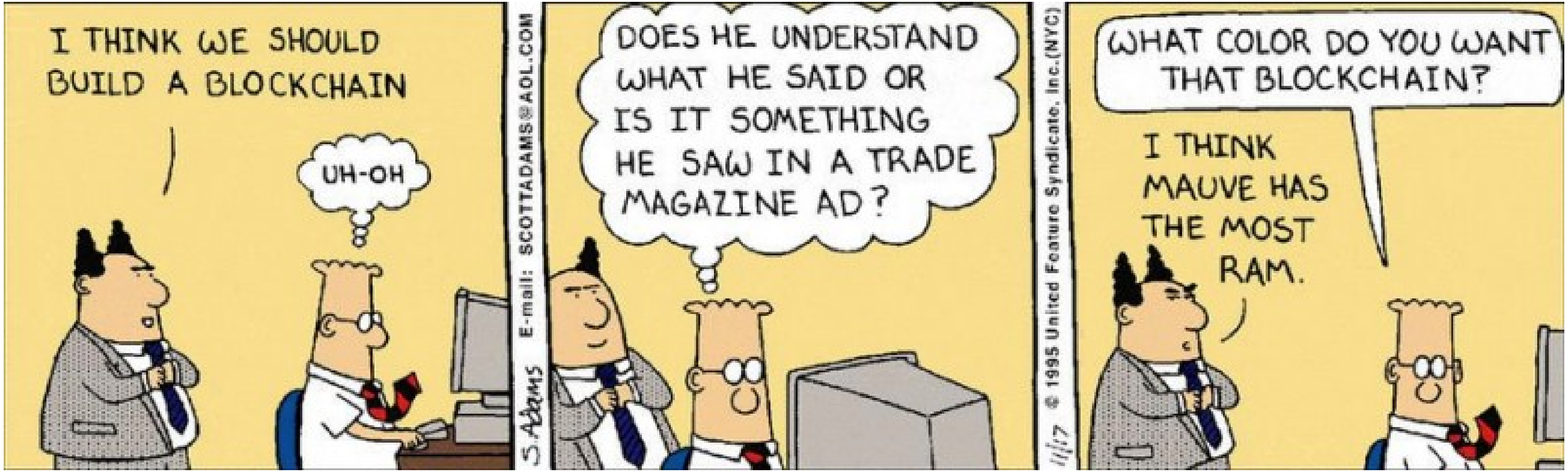
896775 Gen 9 Snappy Cooldown

rabono
Owner

Like 18

https://www.cryptokitties.co/kitty/896775

~~The Mauve Revolution~~


I THINK WE SHOULD BUILD A BLOCKCHAIN
UH-OH
DOES HE UNDERSTAND WHAT HE SAID OR IS IT SOMETHING HE SAW IN A TRADE MAGAZINE AD?
WHAT COLOR DO YOU WANT THAT BLOCKCHAIN?
I THINK MAUVE HAS THE MOST RAM.

S. Adams E-mail: SCOTTADAMS@AOL.COM

11/17 © 1995 United Feature Syndicate, Inc.(NYC)

Common Misconceptions About Bitcoin

✗ Users are anonymous

✗ Every participant has to mine

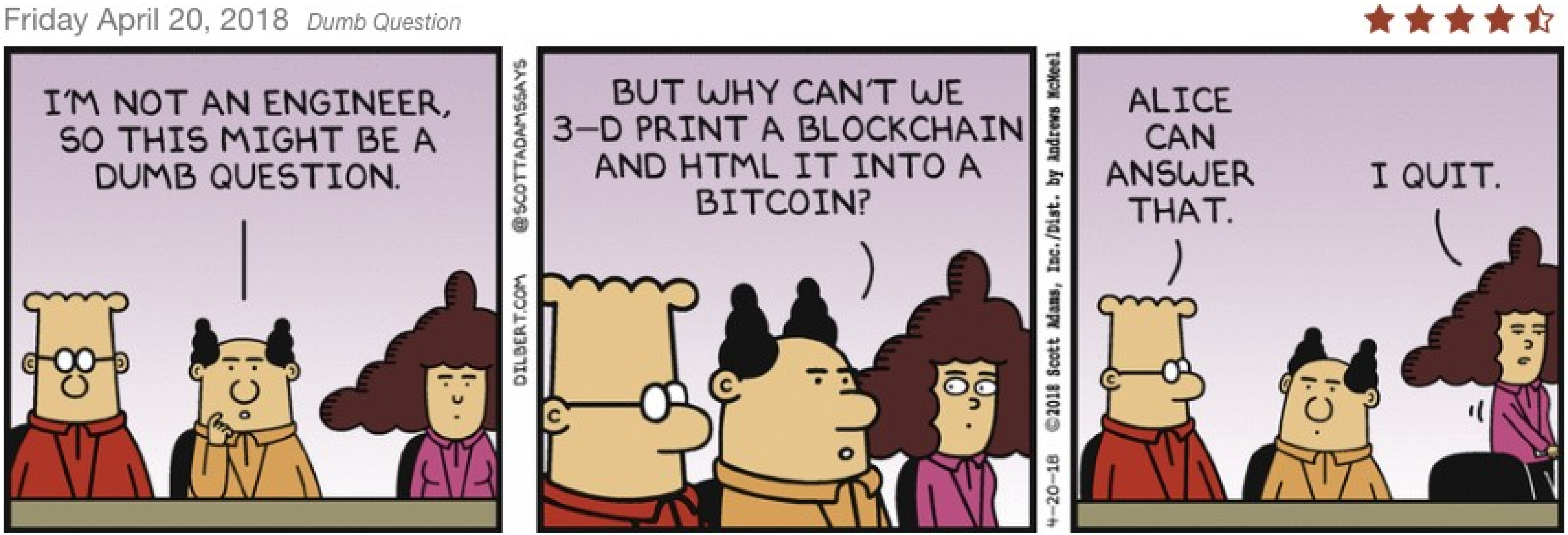
✗ The Blockchain is “encrypted”

✗ Transactions are final

✗ No Trust is Required

Common Misconceptions About Bitcoin

“ If Blockchain is good for Bitcoin,
it must be good for __________ ”



Friday April 20, 2018 *Dumb Question*

I'M NOT AN ENGINEER, SO THIS MIGHT BE A DUMB QUESTION.
@SCOTTADAMSSAYS
DILBERT.COM
BUT WHY CAN'T WE 3-D PRINT A BLOCKCHAIN AND HTML IT INTO A BITCOIN?
©2018 Scott Adams, Inc./Dist. by Andrews McMeel
4-20-18
ALICE CAN ANSWER THAT.
I QUIT.

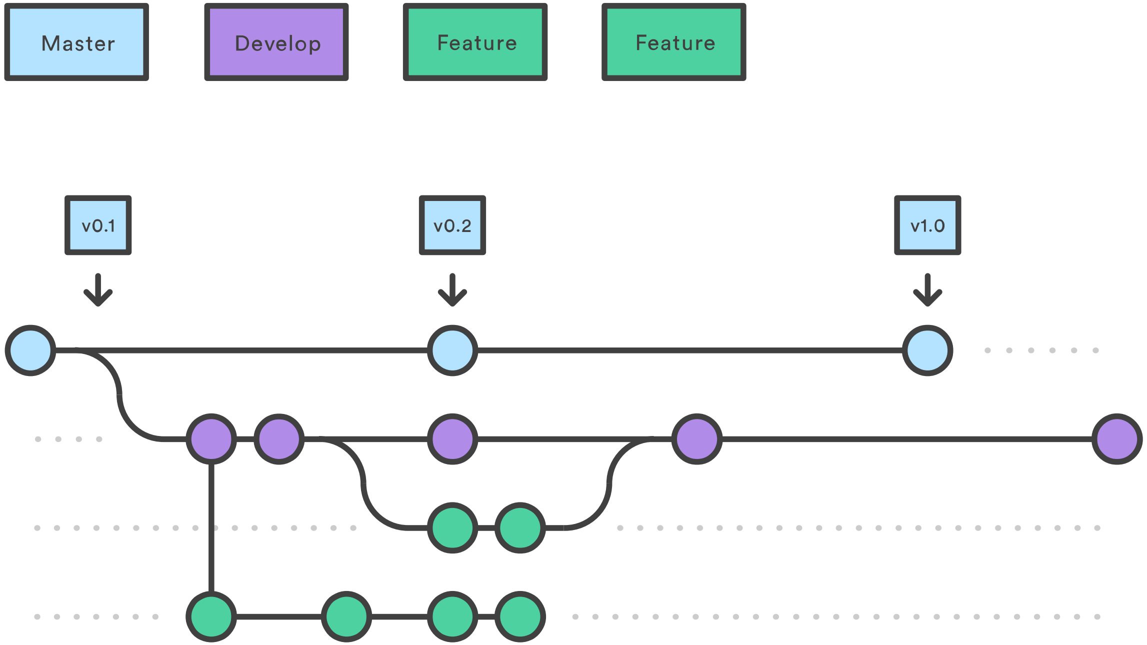
Scott Adams, http://blog.dilbert.com/2018/05/09/all-of-the-dilbert-comics-on-blockchain-bitcoin-or-cryptocurrency/this-might-be-a-dumb-blockchain-question/

What is a “Blockchain”?

- **Still** no agreed upon definition

- *“the actual ledger”*
  - NIST
- *“Linked list with hash pointers instead of pointers”*
  - *Narayanan et al.*
- *Nakamoto Consensus*
  - *Garay et al., Pass et al., etc.*
    … its complicated.

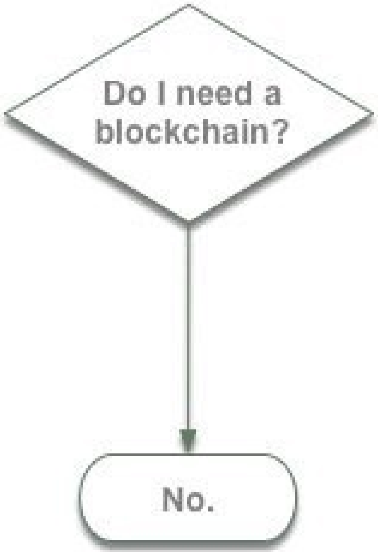
What is a “Blockchain”?



Is GIT a Blockchain?

Blockchain

“A distributed ledger based on an authenticated data structure”

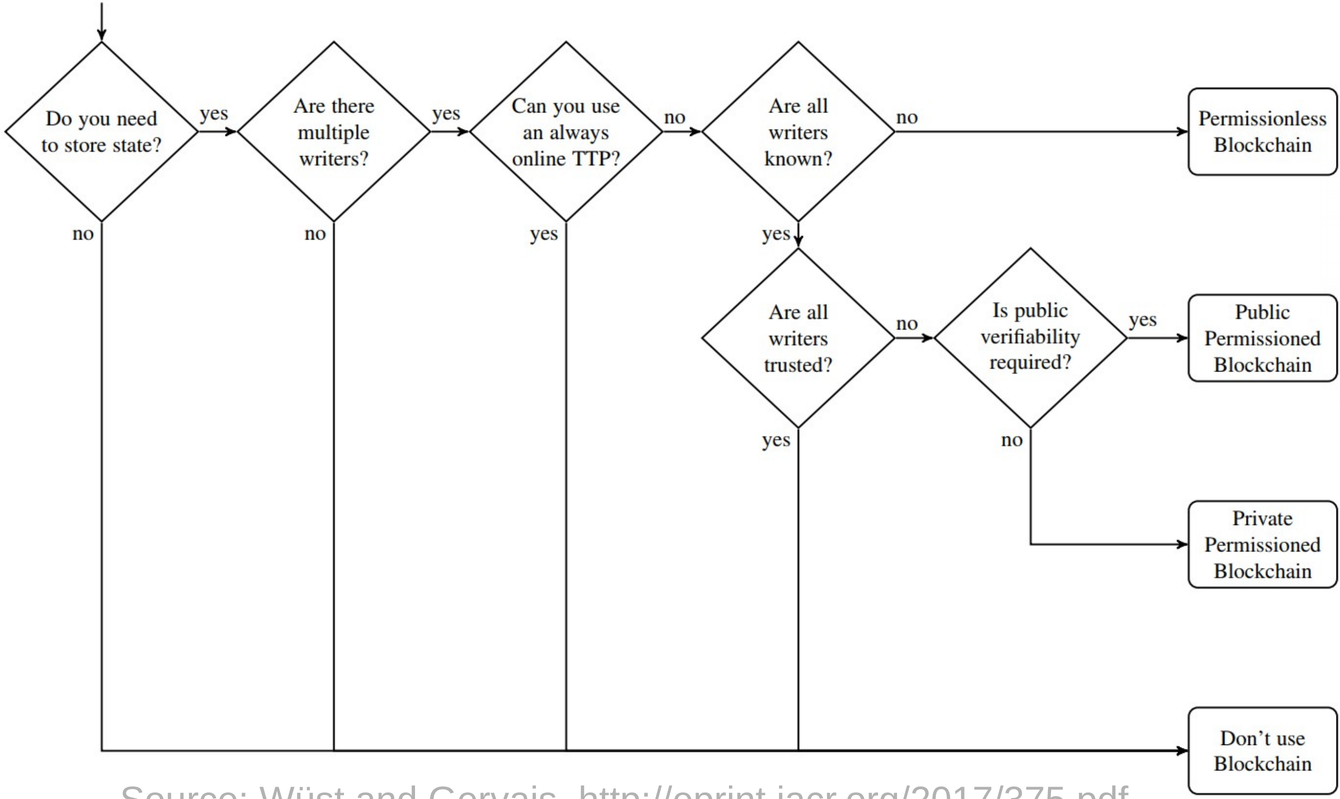


Do I need a blockchain?

No.

[2] http://pngimg.com/download/66321
[3] http://pngimg.com/download/23085

Do I need a Blockchain?


Do you need to store state?
yes
no
Are there multiple writers?
yes
no
Can you use an always online TTP?
no
yes
Are all writers known?
no
yes
Are all writers trusted?
no
yes
Is public verifiability required?
yes
no
Permissionless Blockchain
Public Permissioned Blockchain
Private Permissioned Blockchain
Don't use Blockchain

PoS/X

[2]

BFT

[3]

Source: Wüst and Gervais, http://eprint.iacr.org/2017/375.pdf

*You could accept Cryptocurrencies as a payment option

I need a Blockchain – What could possibly go wrong?

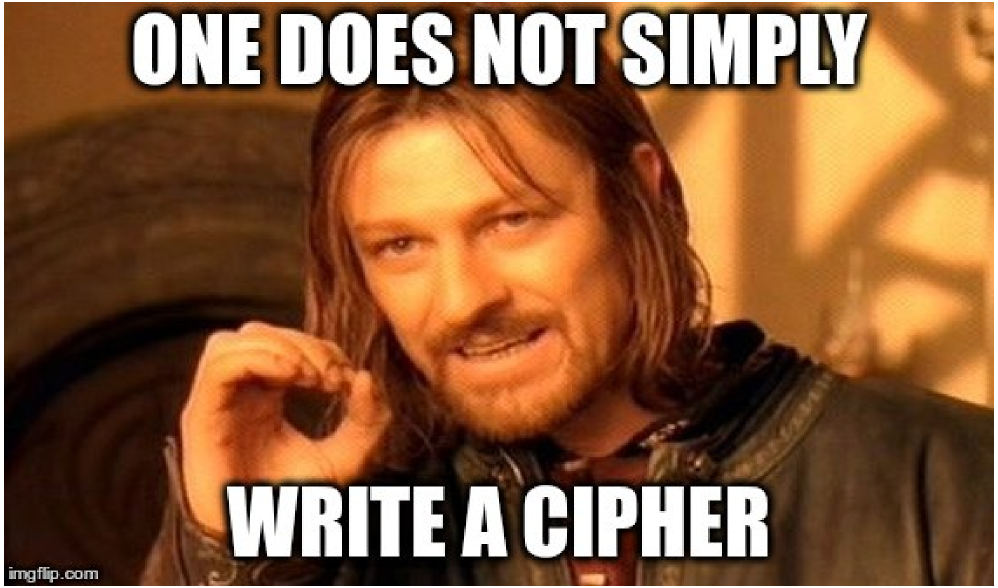
Source: https://twitter.com/JonathanBahai/status/922895017500344320

You’re Doing it Wrong:
Do not use Proof-of-Work

- Security assumptions do not hold for small systems
- Only makes sense in a “permissionless” P2P setting
- If PoW is needed, the design is (probably) flawed

- Also: Do not implement your own consensus protocols
  - Well researched and tested protocols have been available for around 20 years
  - If consensus fails badly your whole system will be affected/broken

You’re Doing it Wrong:
Do not roll your own Cryptography



- Also: Do not use cryptography you do not fully understand

You’re Doing it Wrong:
KISS - “Keep it simple, stupid”

What was needed:

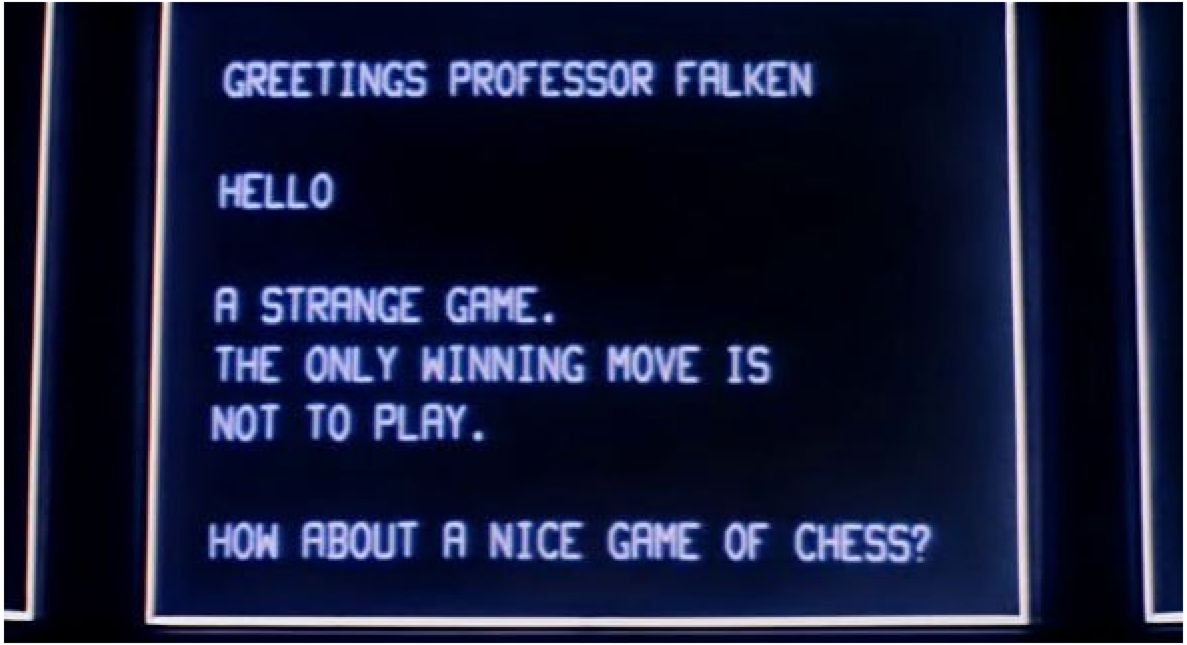
simple time-stamping service to prove a document existed at some point in the past

What was implemented:

decentralized prediction market with an exponentially growing number of tokens that use user-definable Turing-complete spending rules to vote in a decentralized autonomous organization (DAO) on the ordering of time-stamp events which are represented by non-fungible but infinitely divisible quantum resistant time-stamp tokens.*

*Of course the corresponding "white paper" (dark blue text on a black background - it was hard to write it should be hard to read) is so monumental in every conceivable metric that a second ICO had to be started for a new inter-galactic file system which will eventually be capable to actually host the white paper in its entirety.

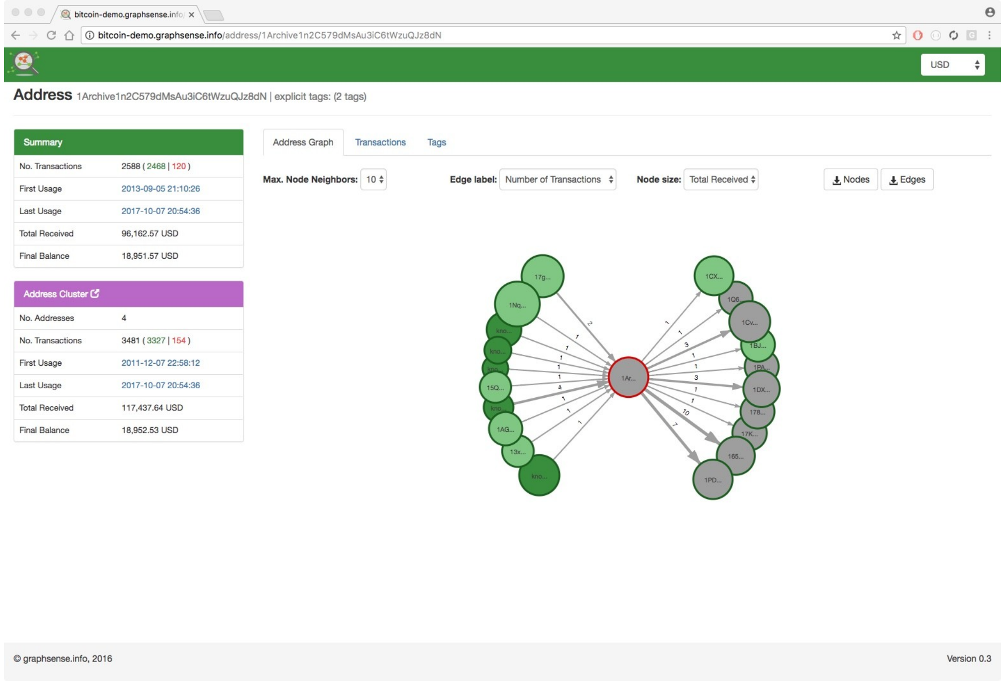
You’re Doing it Wrong:
Cryptoeconomics is your Enemy, not your Friend



```
GREETINGS PROFESSOR FALKEN

HELLO

A STRANGE GAME.
THE ONLY WINNING MOVE IS
NOT TO PLAY.

HOW ABOUT A NICE GAME OF CHESS?
```

Source: WarGames, 1983

You’re Doing it Wrong:
Privacy is hard to get right



bitcoin-demo.graphsense.info

bitcoin-demo.graphsense.info/address/1Archive1n2C579dMsAu3iC6tWzuQJz8dN

USD

Address 1Archive1n2C579dMsAu3iC6tWzuQJz8dN | explicit tags: (2 tags)

Summary	
No. Transactions	2588 (2468 | 120)
First Usage	2013-09-05 21:10:26
Last Usage	2017-10-07 20:54:36
Total Received	96,162.57 USD
Final Balance	18,951.57 USD

Address Cluster	
No. Addresses	4
No. Transactions	3481 (3327 | 154)
First Usage	2011-12-07 22:58:12
Last Usage	2017-10-07 20:54:36
Total Received	117,437.64 USD
Final Balance	18,952.53 USD

Address Graph | Transactions | Tags

Max. Node Neighbors: 10 **Edge label:** Number of Transactions **Node size:** Total Received

© graphsense.info, 2016

Version 0.3

Source: http://graphsense.info

Are Most Blockchain Technologies Bound to Fail?

Roy Lichtenstein, source: https://www.christies.com/

https://en.wikipedia.org/wiki/File:Wheatley.png

“We choose to go to the Moon in this decade and do the other things, not because they are easy, but because they are hard”

John F. Kennedy

Nicholas A. Stifter

nstifter@sba-research.org

10C6 4FD1 19B1 B399 4A2B
6D7B 5EB9 556A 4339 97A9