

Blockchain Technology & Digital Currencies

Poramin Insom (ปรมินทร์ อินโสม) Lead Developer & Founder poramin@zcoin.io

Table of Contents

- Who am I?
- Blockchain Technology
- Blockchain: Financial and Investment Disruption
- Innovative Capitalism : ICO model
- Cryptocurrency
 - Bitcoin
 - Zcoin
 - bubble or homerun?
- Closing and Q&A

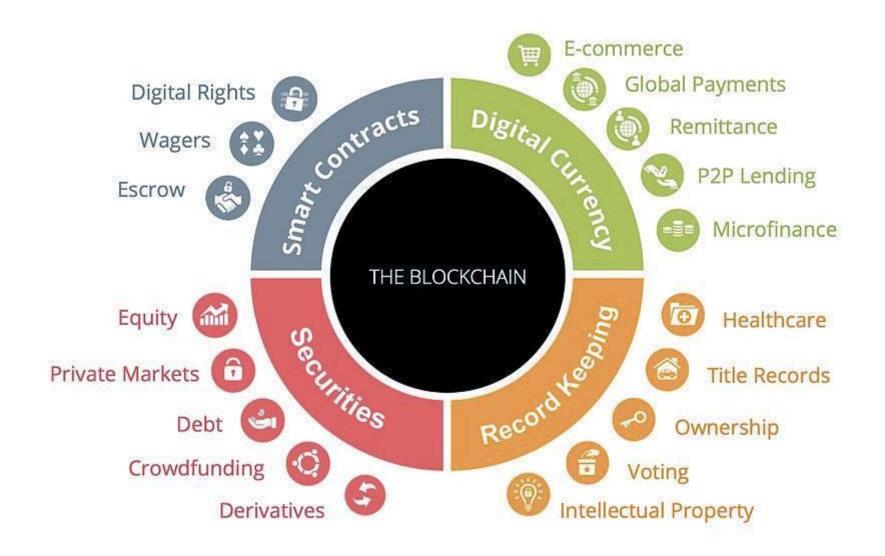
Who am I ?



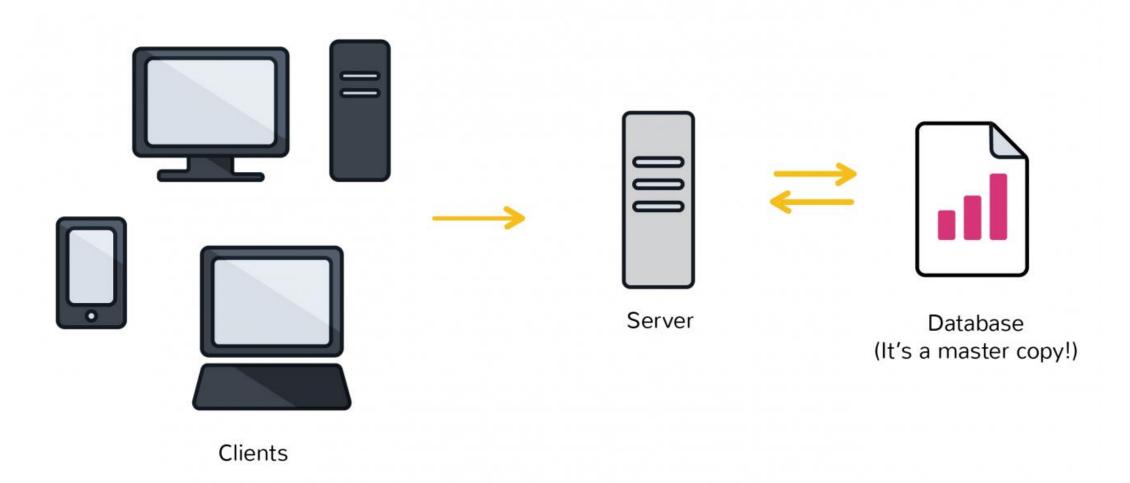
- B.Eng. in Computer Engineering, Second Class Honors, KMITL
- Worked at Microsoft Thailand, Accenture Malaysia
- M.S. in Security Informatics, Johns Hopkins University
- Founder and Core Developer at Zcoin
- Second lieutenant at Cyberwarfare Unit, Royal Thai Armed Forces
- CEO & Co-Founder at Satang Corporation Satang.com and TDAX.com

Blockchain Technology





Z



Disruption in Amazon's cloud service ripples through internet

Jeffrey Dastin 3 MIN READ 9 f



The logo of Amazon is seen at the company logistics center in Lauwin-Planque, northern France, February 20, 2017. REUTERS/Pascal Rossignol

SAN FRANCISCO (Reuters) - Web users experienced widespread glitches on Tuesday, from news sites to government services, after Amazon.com Inc's popular cloud service that hosts their data suffered a technical disruption.





Google apologizes for cloud outage that one person describes as a 'comedy of errors'







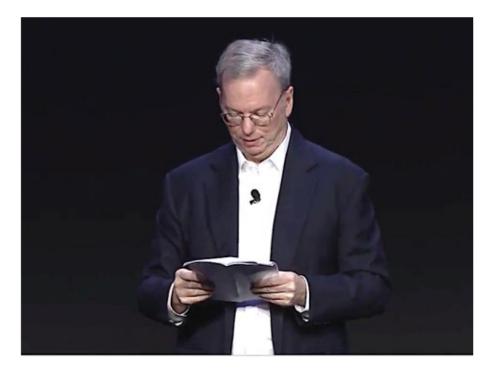






Google is investing billions in its data centers and hiring salespeople like crazy to take on Amazon in the cloud computing industry. It just held a big conference in March to get the IT world excited about its cloud.

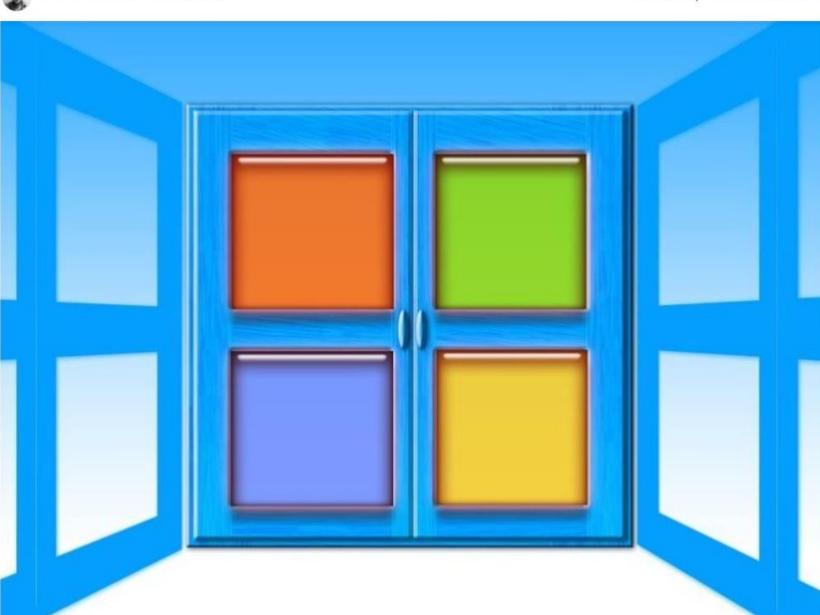
So it was not good that on
Monday, the Google Compute
Engine cloud service went down
for 18 minutes at 7 p.m. Pacific for
just about all of
its customers everywhere.



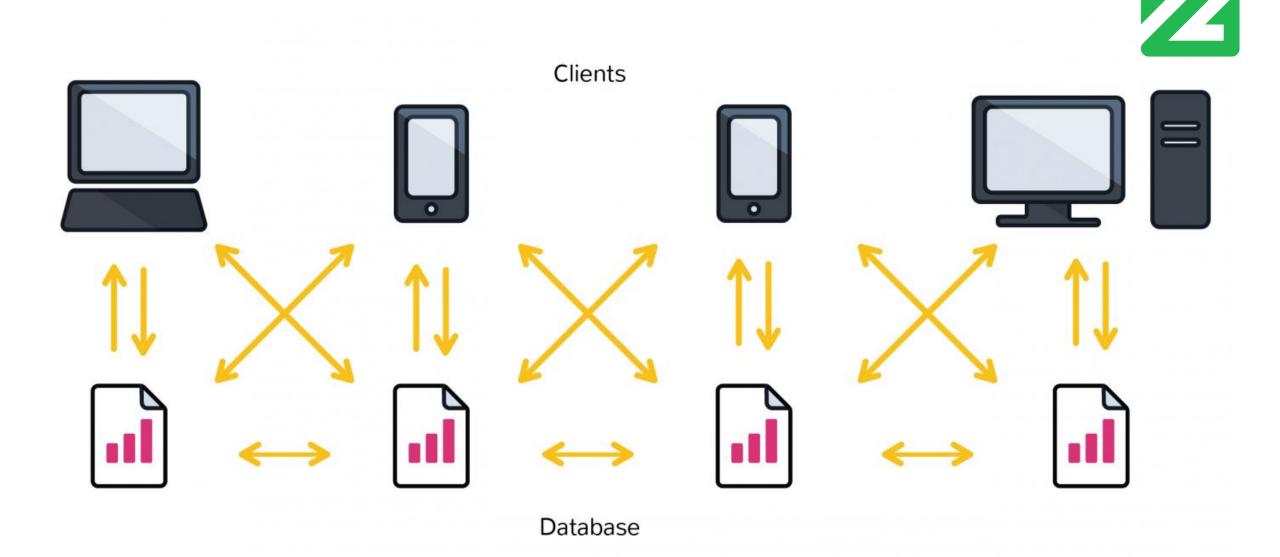
Google executive chairman Eric Schmidt Business Insider

Microsoft down AGAIN: cloud outage pulls Outlook, Xbox and Skype offline TOM BALL - REPORTER - 22ND MARCH 2017 + INCREASE

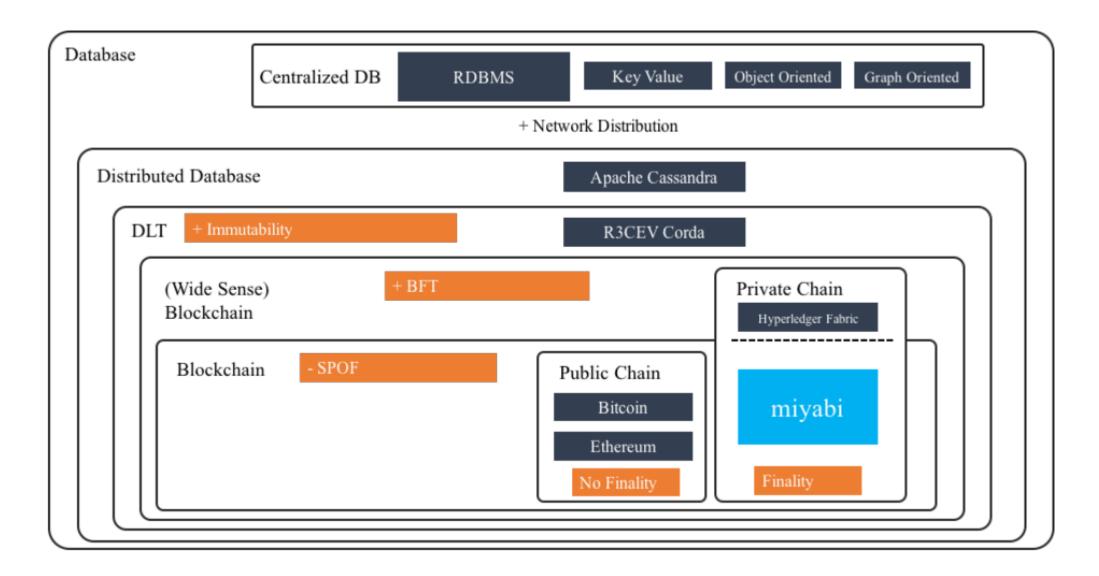
+ INCREASE / DECREASE TEXT SIZE -













Problems

- Outdated
 - (Industries + Paper) in Digital
- Centralized
 - Resistant to change
 - Vulnerable to systems failures and attacks



Solutions

- Outdated
 - (Industries + Paper) in Digital => **Digital Asset**
- Centralized => Decentralized
 - Resistant to change => Majority Vote
 - Vulnerable to systems failures and attacks => No SPOF



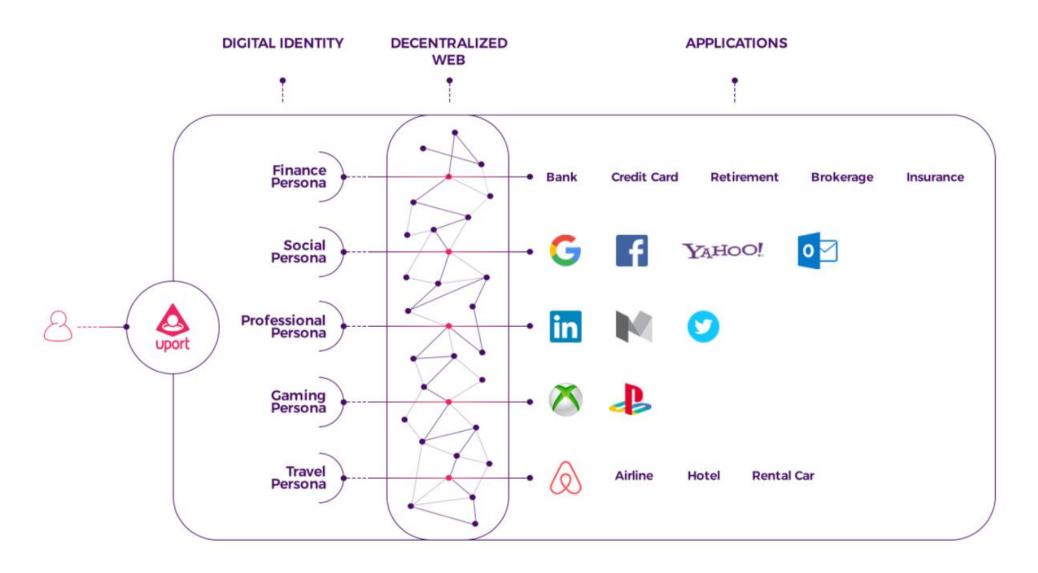
Capabilities

Authenticating Identity and Value => KYC (Know Your Customer)

Be affected!

- Retail banking, Wholesale banking, Investment banking
- Asset managers, Broker dealers
- Payment networks, Lending marketplaces
- Equity crowdfunding
- Regulators and auditors







Capabilities

- Distribution of Value => No single dollar is spent twice
- Be affected!
 - Assets
 - Currency
 - Bonds
 - Diamonds
 - Gold
 - Silver
 - Stocks ...

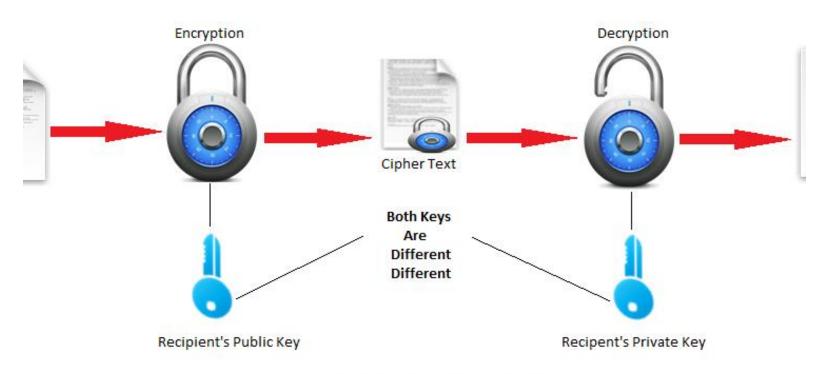






Capabilities

- Storage of Value
- Be affected!
 - Banking institutions

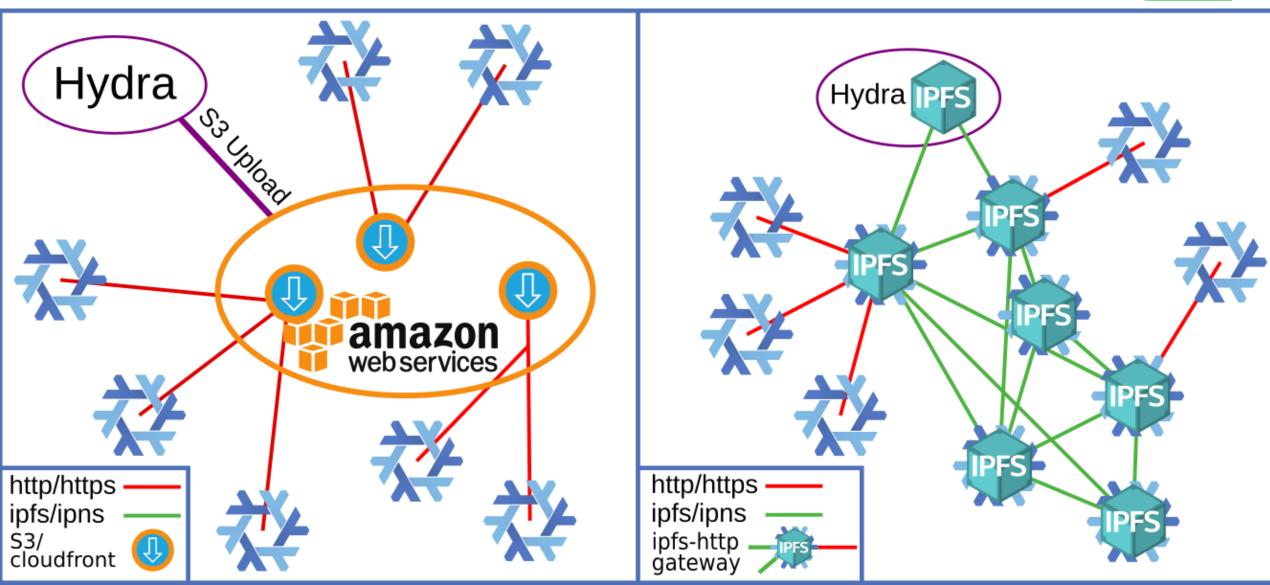


Public Key Encryption





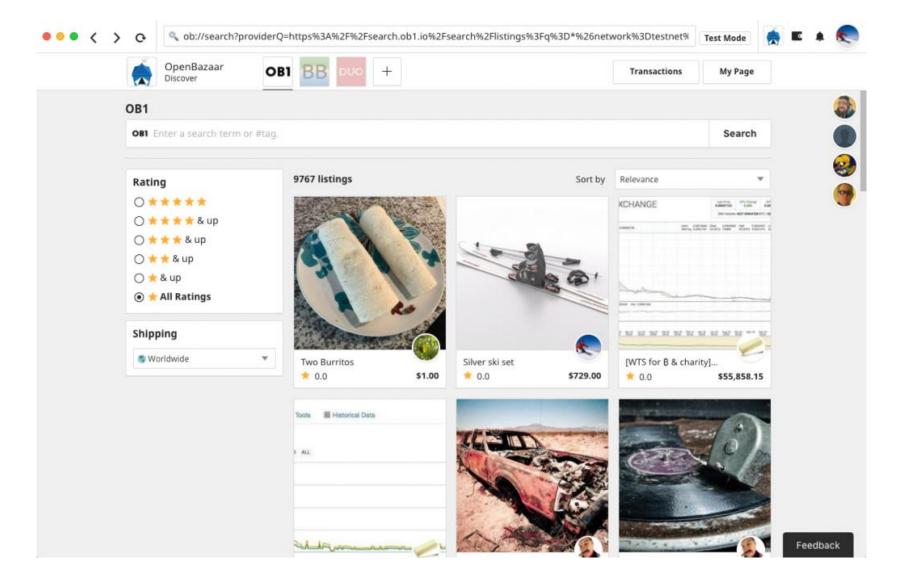






OpenBazaar 2.0 BETA RELEASED





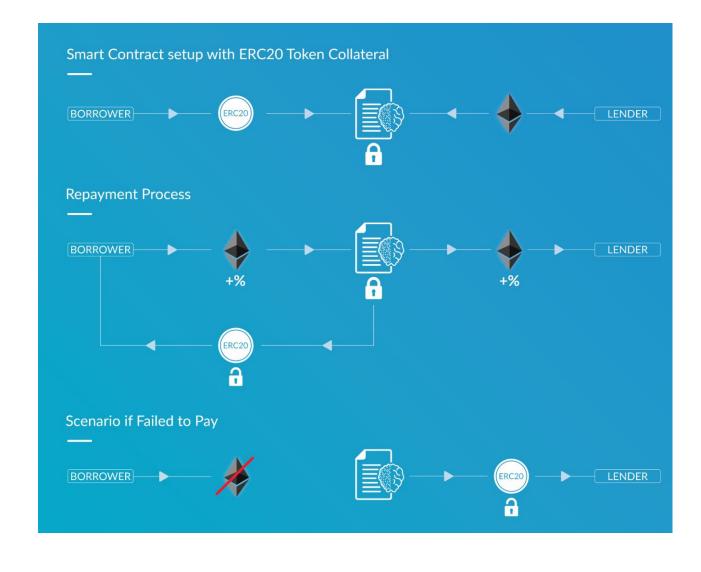




Capabilities

- Lending Value
- Be affected!
 - Banking institutions







Capabilities

- Exchanging Value
- Be affected!
 - Stock Exchange



ETH: BITUSD

BTC: BITCNY

VOLUME:

CHANGE:

228.15822

7,597.168



EXPLORE

EXCHANGE

Welcome to the BitShares DEX

The BitShares decentralized exchange - also known as The DEX - is a next-generation cryptocurrence trading platform.

The DEX is inherently decentralized, enabling you to trade the BitShares core token (BTS) and a rang of trustless price-stable, market-pegged assets such as bitUSD, bitCNY, bitBTC, bitGold and more. These assets can all be traded with zero counter-party risk, putting you in total control of your funds.

The DEX also enables creation of user-issued assets (UIAs), which can be traded against any other UIAs or trustless assets on the platform. One well-known issuer on The DEX is OpenLedger, offering host of assets including BTC, ETH, STEEM, DASH, LTC, DOGE, and many more

This gives cryptocurrency traders a unique blend of traditional and decentralized trading, all in a familiar exchange interface. Happy trading!

CREATE A NEW ACCOUNT

LOGIN WITH PASSWORD

	Top M	1arkets
су		BTS : віт
		PRICE:
	4	VOLUME:
je		CHANGE:
		DASH: E
		DAOII. D
		PRICE:
		VOLUME:
		CHANGE:
a		вітUSD :
	4 5	PRICE:
	USD	VOLUME:
		CHANGE:
		DTe - DT

VOLUME.

CHANGE:

	PRICE:	0.065600 66.09k	B	BTC : BIT PRICE: VOLUME:	USD 3,15
	CHANGE:	τUSD		CHANGE:	: віті
	PRICE: VOLUME: CHANGE:	265.00025 646.020 17.78%	GOLD	PRICE: VOLUME: CHANGE:	1,48
	BITUSD : E	вітCNY	4	ЕТН : віт	CNY
USD	PRICE: VOLUME: CHANGE:	6.24998 315.76к -0.62%		PRICE: VOLUME: CHANGE:	1,32
	BTS:BTC	:		DASH : E	TC

0.926

	вітUSD : в	ытСNY	4	ETH : BIT	CNY	
	PRICE: VOLUME: CHANGE:	6.24998 315.76к -0.62%		PRICE: VOLUME: CHANGE:	1,320.00097 54.84k -11.34%	
	BTS:BTC	:		DASH : B	тс	
<u> </u>	PRICE:	0.00002058		PRICE:	0.07951841	
•	VOLUME:	31.226		VOLUME:	0.038	
	CHANGE:			CHANGE:		
	STEEM : E	втс		вітСМҮ :	BTS	
	PRICE:	0.00030450	22	PRICE:	2.49931	

SOLD	PRICE: VOLUME: CHANGE:	1,481.48148 55.008 4.64%		PRICE: VOLUME: CHANGE:	144.00000 950.226 -0 10%	B	PRICE: VOLUME: CHANGE:	19,799.79092 252.20к -7.72%	
<u> </u>	ЕТН : віт	CNY		YOYOW:	вітСNY		ОСТ: вг	TCNY	
	PRICE:	1,320.00097	(~~~	PRICE:	0.15290	()	PRICE:	0.77194	
₹ .	VOLUME:	54.84ĸ		VOLUME:	228.06ĸ		VOLUME:	57.00ĸ	
	CHANGE:			CHANGE:			CHANGE:		
	DASH : B	тс		OBITS : BTC			BLOCKPAY : BTC		
- 7)	PRICE:	0.07951841		PRICE:	0.00015000		PRICE:	0.00003842	
	VOLUME:	0.038		VOLUME:	0.177	N. A. V.	VOLUME:	0.702	
	CHANGE:			CHANGE:			CHANGE:		
	BITCNY: BTS		\blacksquare	ETH: BTS			HERO : BTS		
	PRICE:	2.49931		PRICE:	3,399.00525	[112-403]	PRICE:	2,141.00000	
CNY	VOLUME:	17.13м		VOLUME:	375.11ĸ		VOLUME:	26.43K	
	CHANGE:			CHANGE:			CHANGE:		

USDT: BITUSD

HERO: BITUSD

0.88900

655.693

PRICE:

VOLUME:

CHANGE:

3 152 30122

BITUSD

14.40k

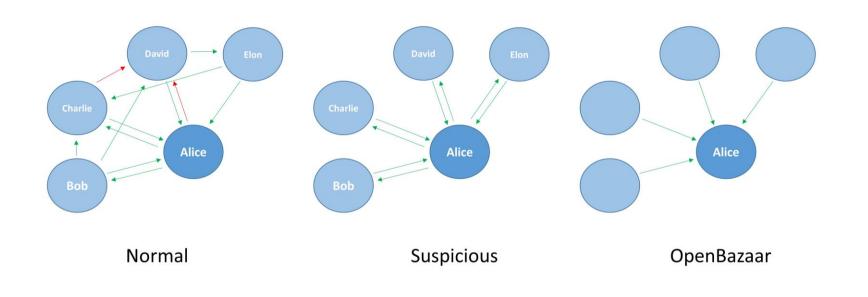


Bitsquare	are															_ [) ×
Market	Buy BTC	Sell BTC	Portfolio	Funds	Support			H/BTC: 0.009! price (Ask)	54401	POLONIEX	0.00 BTC Available balan		0.00 BTC Reserved in offers		.00 BTC ced in trades	Settings	Account
Sell bit	tcoin Ta	ke offer	Crea	te offer×													
Sele	ct tradin	g accou	nt —														
	Tr	ading acc	ount:	ETH: 0xc1	lb8 (ETH, Al	tcoins)	•										
		Curr	ency:	Ether (ET	H)												
┌ Set a	amount a	and pric	e														
	,	_		Amount of	f bitcoin to sell		Price in B	BTC for 1 ETH				An	nount in ETH to re	eceive			
		~			0.10	втс		0.0095	втс	Fixed	Percentage	=		10.53	ETH		
				Minimum ar	mount of bitcoin		Distance in	% from market	price								
	Sell bi	itcoin			0.10	втс		0.23	%								
Fund	Trade	nds need	dress:	0.1107 BT 18qLayrG 0.00 BTC	rC Zy6EK5oyK3e	ZpQL9nRI	HSPytbzP								ර ම රි		7.0 7.0 7.0 7.0 7.0 7.0 7.0 7.0 7.0 7.0
				Transfer f	unds from Bits	square wa	or OR	Open your ex	ternal	wallet f	for funding	W	aiting for funds				

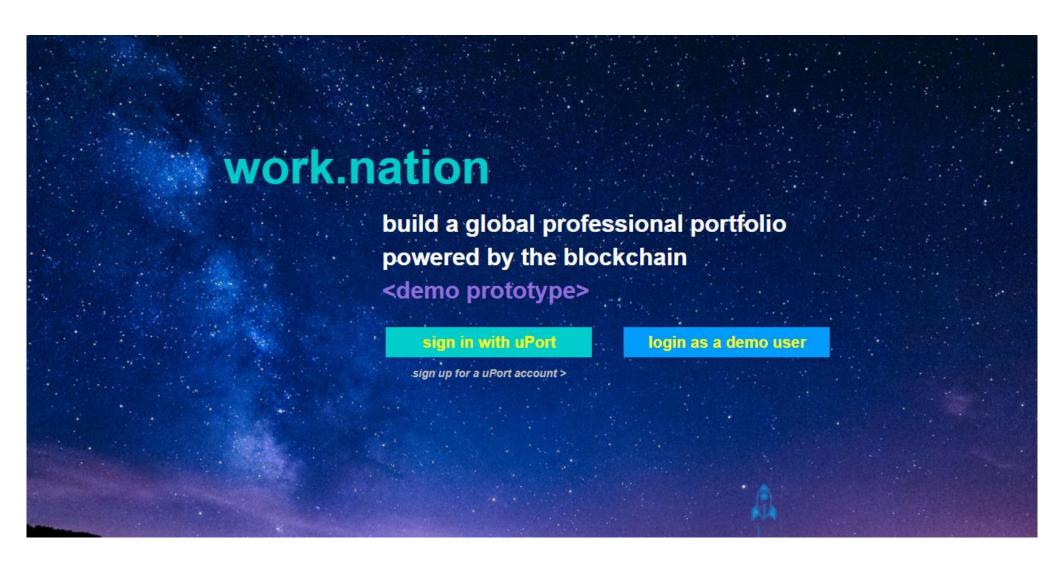


Capabilities

Insuring Value and Managing Risk => Blockchain Reputational Systems











Closed initial coin offerings greater than or equal to \$500K. 2014 - YTD (9/8/2017)



Tezos' \$232 Million ICO May Just Be The Beginning



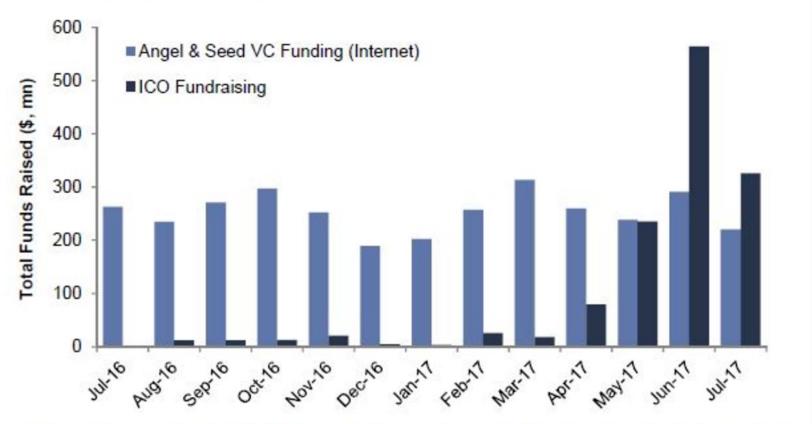






Exhibit 8: The pace of ICO fundraising has now surpassed Angel & Seed stage Internet VC funding globally

Total Funds Raised by month (\$, millions)



Note: ICO fundraising as of July 18th, 2017, per Coin Schedule. Angel & Seed VC funding data as of July 31st, 2017 and does not include "crowdfunding" rounds.

Source: CoinSchedule, CB Insights, Goldman Sachs Global Investment Research.



Preamble

EIP: 20

Title: ERC-20 Token Standard

Author: Fabian Vogelsteller <fabian@ethereum.org>, Vitalik Buterin <vitalik.buterin@ethereum.org>

Type: Standard Category: ERC Status: Accepted Created: 2015-11-19

b Simple Summary

A standard interface for tokens.

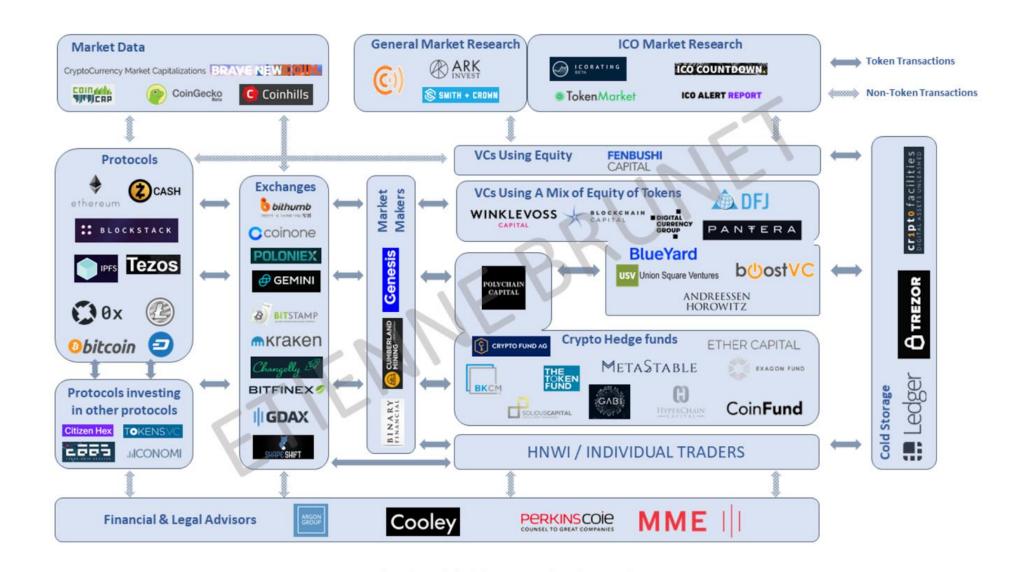
Abstract

The following standard allows for the implementation of a standard API for tokens within smart contracts. This standard provides basic functionality to transfer tokens, as well as allow tokens to be approved so they can be spent by another on-chain third party.

Motivation

A standard interface allows any tokens on Ethereum to be re-used by other applications: from wallets to decentralized exchanges.









Buy: 126,751.80 THB | Sell: 120,981.00 THB Buying & Selling How It Works Security Terms & Privacy ภาษาไทย

Bitcoin network may encounter potential hardfork on 31st July - 1st August 2017. Please don't send or receive Bitcoins during 29th July - 2nd August 2017.

Bitcoin Made Social!

Make and share payments to friends with Bitcoin









Download Presentation

Our presentation for Blockchain meetup at Microsoft Thailand can be download here.

Social

Find your friends, see who are nearby, send and request to them at anywhere and anytime!

Real-time

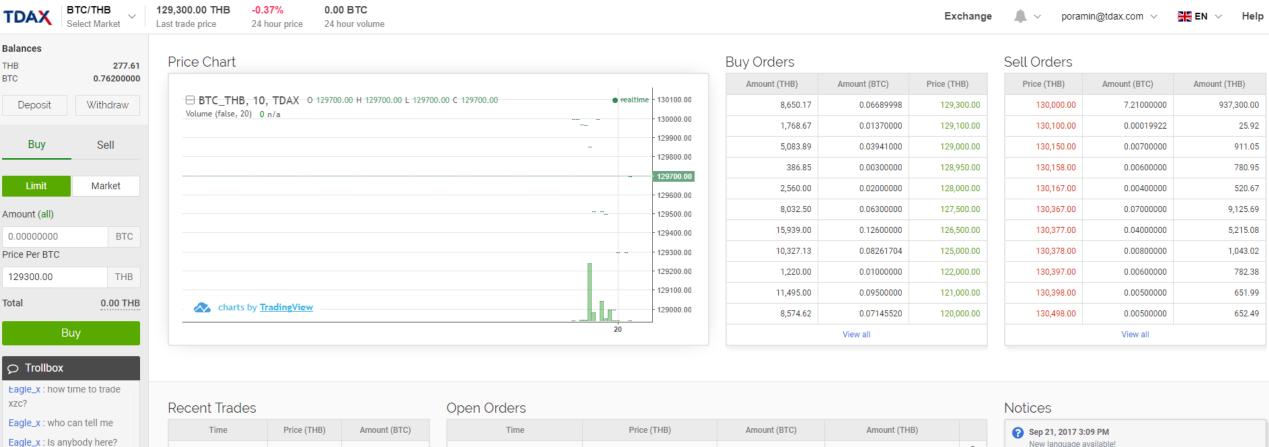
Everything is on real time. See your feeds live update, get notifications when something is done, and so on. Watch it live updates at the right side!

Secure

We put security as our top priority. Just for you! See Security.







tecent mades							
Time	Price (THB)	Amount (BTC)					
✓ 13 hours ago	129,300.00	0.00050001					
↑ 13 hours ago	130,100.00	0.00050001					
→ 13 hours ago	129,300.00	0.00050001					
↑ 13 hours ago	130,100.00	0.00030077					
↑ 13 hours ago	130,100.00	0.00019924					
^ 2 days ago	129,300.00	0.00100000					
^ 2 days ago	129,000.00	0.00100000					
✓ 2 days ago	129,000.00	0.01959000					
✓ 3 days ago	129,500.00	0.00500000					
✓ 3 days ago	129,515.00	0.03541000					
View all							

anuith: they said XZC is coming in about a month

Guest555 : ..

Enter Messages

anuith: in a news somewhere

1

Time	Price (THB)	Amount (BTC)	Amount (THB)	
Sep 21, 2017 12:55 PM	130,000.00	7.21000000	937,300.00	ŵ
Sep 19, 2017 9:25 AM	130,800.00	0.00700000	915.60	ŵ
Sep 19, 2017 9:24 AM	130,500.00	0.00600000	783.00	ŵ
Sep 19, 2017 9:24 AM	130,498.00	0.00500000	652.49	î
Sep 19, 2017 9:24 AM	130,398.00	0.00500000	651.99	î
Sep 19, 2017 9:23 AM	130,397.00	0.00600000	782.38	î
Sep 19, 2017 9:22 AM	130,378.00	0.00800000	1,043.02	Û
Sep 19, 2017 9:22 AM	130,377.00	0.04000000	5,215.08	ŵ
Sep 19, 2017 9:21 AM	130,367.00	0.07000000	9,125.69	î
Sep 19, 2017 9:21 AM	130,167.00	0.00400000	520.67	Û
	View	all		

New language available! We have added Chinese language:).

Sep 21, 2017 12:49 AM

เราได้ทำการยืนยันตัวตนและบัญชีธนาคารผู้ใช้ส่วนใหญ่แล้ว! หากผู้ใช้งานท่านใดยังคงไม่ได้รับการตรวจสอบ รบกวนทักแชทเพื่อให้ เจ้าหน้าที่แจ้งข้อผิดพลาดของการตรวจสอบครับ

2 Sep 19, 2017 11:35 AM เรียนผู้ใช้ที่เคารพทุกท่าน เนื่องจากในขณะนี้มีผู้สมัครเข้าใช้งานเป็นจำนวนมาก ทำให้การยืนยันตัว ตนและบัญชีธนาคารอาจเกิดความล่าช้าไปบ้าง ทางทีมงานต้องขออภัย ในความไม่สะดวกเป็นอย่างสูงครับ โดยทางทีมงานจะรีบดำเนินการ ยืนยันอย่างเร็วที่สด

Sep 19, 2017 9:09 AM Hello users, happy trading:) Open at 9.09



Z

- SEC: Virtual Tokens Issued in Blockchain-Based ICO's may be "Securities"
- According to Chinese Official, China's Ban on Initial Coin Offerings is Only Temporary
- มุมมองของ ก.ล.ต. กรณี ICO (http://www.sec.or.th/TH/Pages/FinTech/ICO.aspx)

"ก.ล.ต. มีนโยบายส่งเสริมการเข้าถึงทุนของธุรกิจ ซึ่งรวมถึงกลุ่มเทคสตาร์ทอัพที่มีศักยภาพ และเห็นว่า ICO สามารถเป็น กลไกที่ช่วยตอบโจทย์เรื่องการระดมทุนให้ธุรกิจดังกล่าวได้ ทั้งนี้ หาก ICO ใดมีลักษณะที่เข้าข่ายเป็นหลักทรัพย์ ผู้ระดมทุนก็ ต้องดำเนินการตามกฎหมาย / กฎเกณฑ์ที่เกี่ยวข้องด้วย

อย่างไรก็ดี ก.ล.ต. ยอมรับว่าการทำธุรกิจของกลุ่มเทคสตาร์ทอัพมีความแตกต่างจากธุรกิจในรูปแบบที่คุ้นเคย และการ ระดมทุนลักษณะดังกล่าวอาจไม่สอดรับกับเกณฑ์การกำกับดูแลหลักทรัพย์ที่มีอยู่ในปัจจุบัน ก.ล.ต. จึงอยู่ระหว่าง พิจารณาแนวทางการกำกับดูแลที่เหมาะสม และยินดีรับฟังทุกความเห็นจากภาคธุรกิจ เพื่อไม่ให้มีกฎเกณฑ์ที่เป็นอุปสรรค ต่อการสร้างนวัตกรรมที่เป็นประโยชน์ ในขณะที่ยังสามารถป้องกันไม่ให้ผู้ที่ไม่สุจริตอาศัยช่องทางนี้หลอกลวงเงินจาก ประชาชน"







Public

(i) Sale [65.1% of OMG issued]

The bulk of the OMG will be released in a sale, where they will be sold in exchange for up to a maximum of USD \$25 million equivalent.

(ii) Airdrop [5% of OMG issued]

We will airdrop 5% of OMG tokens to ETH stakeholders, as a means to encourage incentive alignment with the Ethereum mainnet, with which the OmiseGO chain will have a symbiotic relationship, and which will promote the diversity and balance of our PoS network validators. Airdrop will take place after the closing of the crowdsale. It is by no means a way to solicit funding for the sales. Further information about airdropping can be found in the Explanatory Note & Governance Term.

Private

(iii) OmiseGO reserve [20% of OMG issued]

Directly released by the smart contract to OmiseGO for future costs and uses including use for network validation as part of the development and execution of the project. These OMG are locked through a smart contract function and may not be transacted by OmiseGO for a period of 1 year, starting at the end of the creation period.

(iv) Team [9.9% of OMG issued]





Joseph Poon
Lightning Network Co-Author
OmiseGO Principal Author



Vitalik Buterin Founder of Ethereum Proof-of-Stake Research: Scalability, Safety, Privacy



Co-Founder of Ethereum, Founder of Parity & Polkadot Consensus Technology Research, Development and Utilization

Dr. Gavin Wood



Jae Kwon

Creator of Tendermint, and Cosmos Network Proof-of-Stake Research - BFT Consensus, Speed, Interoperability



Vlad Zamfir

Casper (Ethereum) Research Lead

Proof-of-Stake Research:
Economic Security, Consensus

Protocols, Correct-byConstruction Protocols



Martin Becze
eWASM (Ethereum Web
Assembly) creator
Scalability research: eWASM,
VM's, microkernels



Julian Zawistowski
Founder of Golem
Decentralised Economics
Enthusiast



Prof. David Lee Kuo Chuen
Professor of Quantitative Finance,
Singapore University of Social
Sciences
Financial Inclusion, Microfinance



Pandia Jiang
Founder of LinkTime
Community Relations, CryptoBusiness Advisor



Roger Ver
CEO of bitcoin.com, First Major
Backer of Earliest Crypto Startups
Decentralization Advisor, Human
Rights Advocate





DISRUPT SF TechCrunch's flagship event begins next week - don't miss out **Get your tickets today**

initial coin offering

Popular Posts



Facebook's generation of 'lew Hater' and other advertising categories prompts system inspection



Social Capital to take startups public without an IPO





Reid Hoffman on evolving product-market fit and sizing up talent



The promise of identity on the blockchain



Mercedes-Benz will electrify its entire car lineup

The first ICO unicorns are here

Posted Aug 31, 2017 by Jon Russell (@jonrussell)





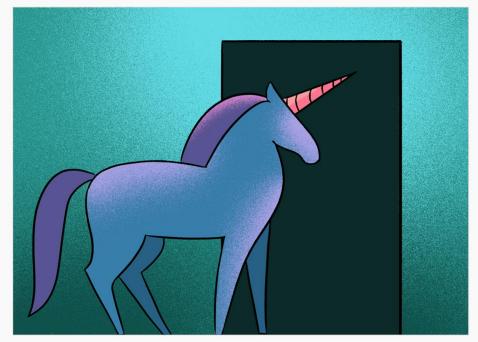






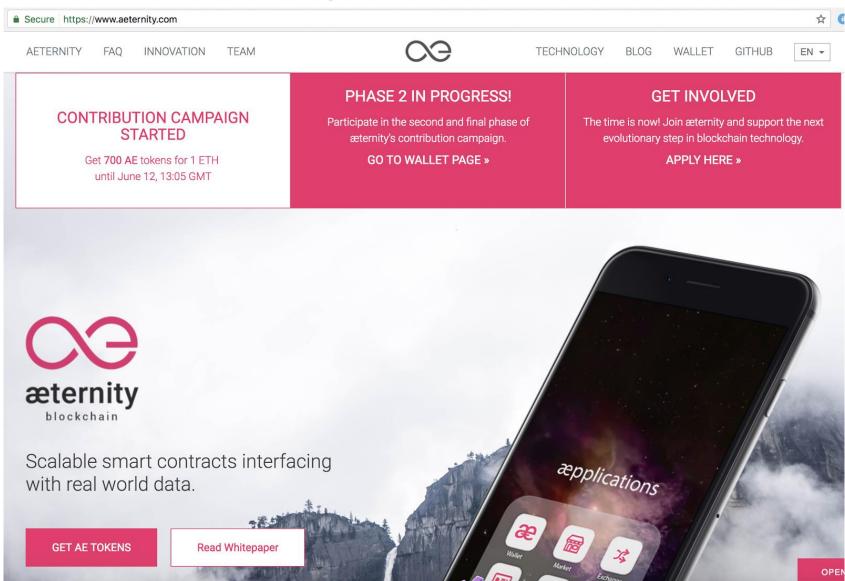






It was always likely to happen, but the speed in which the first ICOs worth more than \$1 billion have arrived is surprising.

Today both OmiseGO (OMG) and Qtum passed a \$1 billion market cap today, according to coinmarketcap.com, a site that tracks the value of crypto tokens. In doing so, they







Starting from a savvy critique of the smart contracts of **Ethereum** and other modern platforms, it is born the new initiative of the self-proclaimed godfather of **Ethereum**, Yanislav Malahov, **Aeternity**, which seeks to integrate the best aspects of the main platforms into one **blockchain**. According to Malahov, he and Vitalik Buterin - founder of **Ethereum** - maintained labor exchanges for a development based on **blockchain** that later would decant in

28 Augur \$189,922,700 \$17.27 11,000,000 REP * \$789,027 -2.02%

Malahov, along with **Augur's** ex-developer Zack Hess and computer maker Jack Pettersson, has decided to outbid **Ethereum** and other platforms such as *Namecoin*, *Truthcoin* and *Factom* with the creation of **Aeternity**. In the whitepaper of this new platform, they give account of all the advances made by these companies. However, they note that all have failed to unify all these benefits, also having deficiencies in governance issues, scalability, scripting, security or cheap access to the real-world data. The goal of **Aeternity** is to improve all these aspects.



107



Zack(creator) of Aeternity on why he left github.com submitted 12 days ago by mcmike313 114 comments share report

ALL 114 COMMENTS

SORTED BY: BEST (SUGGESTED) ▼

[-]



∧ airmc Moonbull 13 points 12 days ago

Deary me, is this real? Surely it can't be real. I mean, no way, right?

... Right? Guys?

permalink embed report

giricrak 7 points 12 days ago*

I posted this below, posting here for some more info/perspective

Disclaimer: I did participate in Ae's ico.

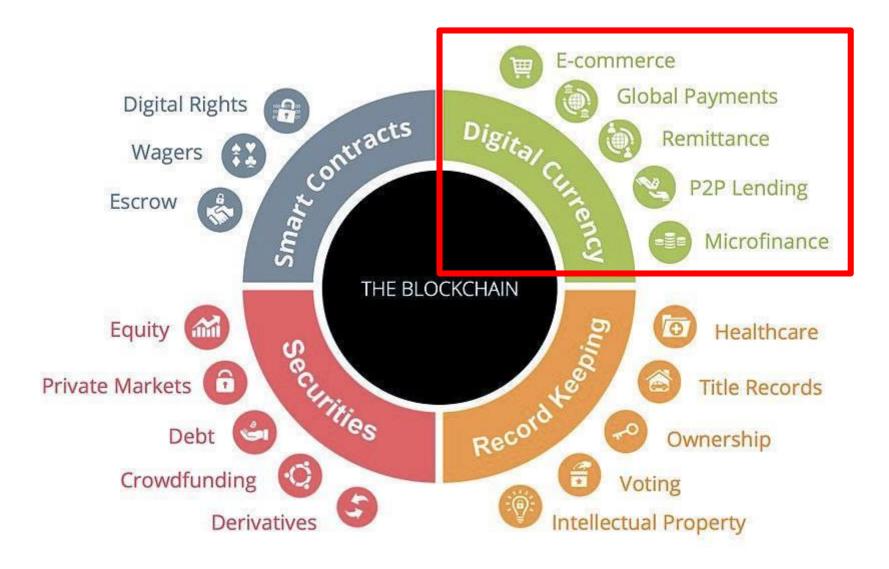
Zack's reddit account is /u/ agorism1337





Digital Currencies





What is Cash?



- **NOTE:** It is a piece of paper with certain amount written on it and a probably a serial number written on it.
- COIN: It is a piece of metal, mostly circular in shape with certain amount depicted on it.





What is Electronic Cash (E-cash) ?



- It is a file having some code or sequence of number.
- This file is transferable from one network to another network.

















微信支付

Account Based Approach



















- A third party maintains a database of various accounts and for transactions, simply deduct money from one account and add to another account.
- They get paid for providing services.
- Example: Bank System.

Account Based Approach : Disadvantages

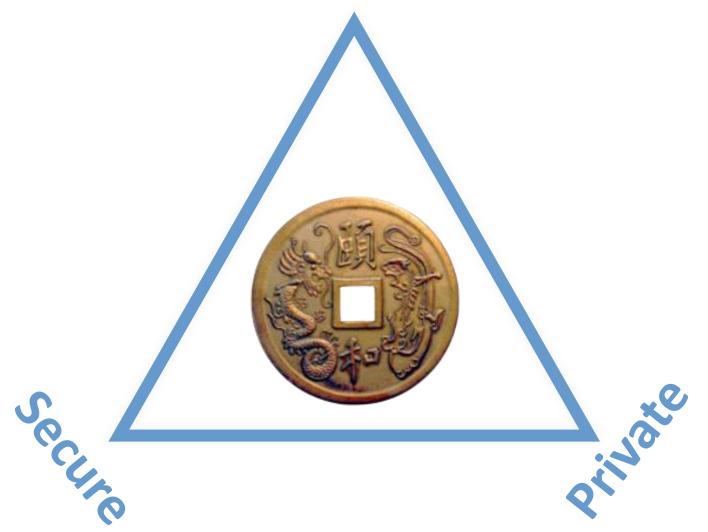


- Trusted parties required to operate.
- Centralization and Trust.
- Money can be stolen. (Robbery)
- Bank can go out of business. (Bankrupt)
- Privacy issue. (Your data can be sold)
- Your account can be seized.



An Ideal Digital Currency





Bitcoin

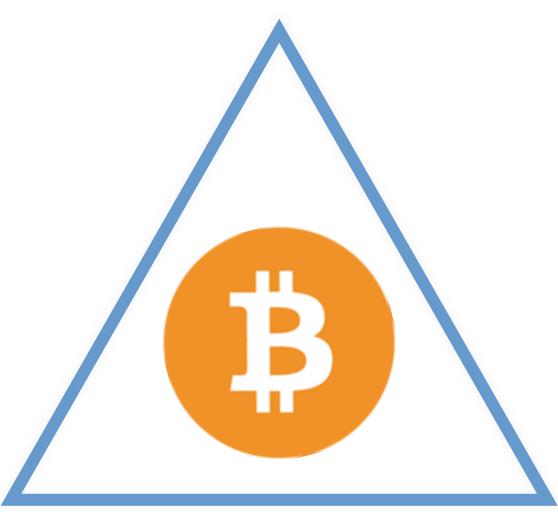
- A distributed digital currency system
- Released by Satoshi Nakamoto 2008
- Market cap of 70 Billion USD (larger than PayPal)
- Effectively a bank run by an ad hoc network
 - A distributed transaction log

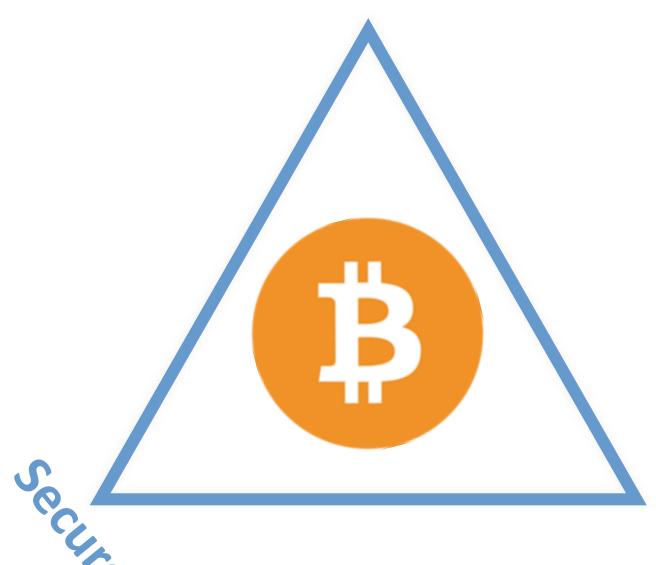


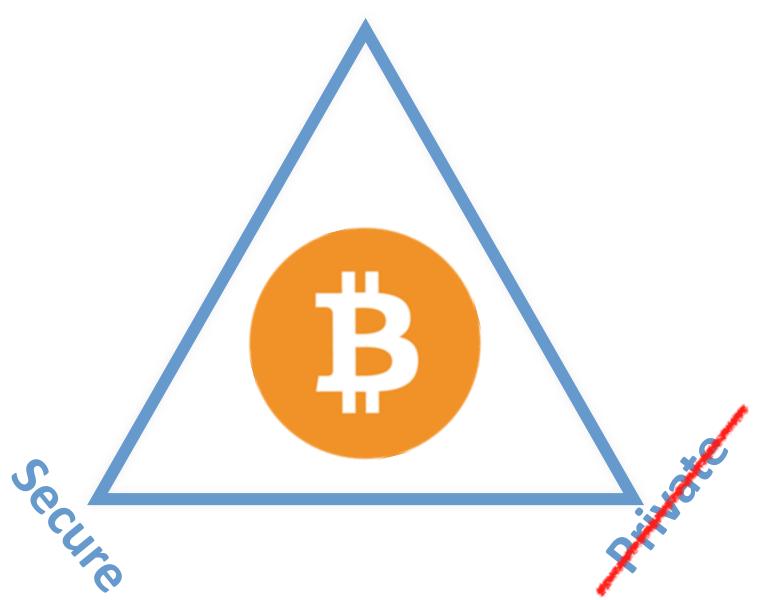
Source: Nasdaq.com

***** 50,091,648,513

Source: CoinMarketCap.com







Evaluating User Privacy in Bitcoin Evaluating User Privacy in Bitcoin (Application of the privacy of the priv

Quantitative Analysis of the Full Bitcoin Transaction Graph

Dorit Ron and Adi Shamir

Department of Computer Science and Applied Mathematics, The Weizmann Institute of Science, Israel {dorit.ron, adi.shamir}@weizmann.ac.il

example of a large scale global blich accessible (but



An Analysis of Anonymity in the Bitcoin System

Quantitat

Departr

This blog is written by Fergal Reid and Martin Harrigan. We are researchers with the Clique Research Cluster at University College Dublin. The results in this blog are based on a paper we wrote that considers anonymity in the Bitcoin system. A preprint of the paper is available on arXiv.

Update (January 1, 2013): We received many requests for an up to date, human-readable copy of



Bitcoin: all of your information is known to the bank the merchants EVERYONE



The Zcoin Project

Brief Introduction of Privacy Centric Cryptocurrency

What is Zcoin?

Zcoin is considered an Altcoin or Alternate Coin

Alt coin is any cryptocurrency that is NOT Bitcoin

Bitcoin is provides a platform for value and liquidity for alt coins

Altcoins are trying to expand the capability of Bitcoin



Zcoin 1st Class Privacy Solution



Zcoin is based on Bitcoin Core code and adopts the same 21 million supply and 4 year coin emission halving

There has been advancements in Blockchain Forensics and USA and EU govt programmes to link Bitcoin transactions to individuals or groups of individuals

Zcoin is here is solve the PRIVACY PROBLEMS of the bitcoin network

Zcoin Privacy Technology

Zcoin is the first implementation of Zerocoin paper written by a team of cryptographers at John Hopkins University in 2016.

Zero Knowledge Proof allows the 'burning' of a token and a 'creation' of a brand new token without transaction history

A major improvement beyond 'coin mixing'

Zcoin has an anonymity set that encompasses all minted coins in a particular RSA accumulator that can scale to many thousands and not subject to transaction graph analysis.





JPMorgan CEO Jamie Dimon says bitcoin is a 'fraud' that will eventually blow up

- "It's worse than tulip bulbs. It won't end well. Someone is going to get killed,"
 Dimon said.
- Bitcoin fell to trade around its session lows after Dimon's comments.
- Dimon's criticism comes at a time when some well-known figures on Wall Street are starting to embrace the cryptocurrency.

Fred Imbert | @foimbert

Published 1:27 PM ET Tue, 12 Sept 2017 | Updated 4:39 PM ET Tue, 12 Sept 2017





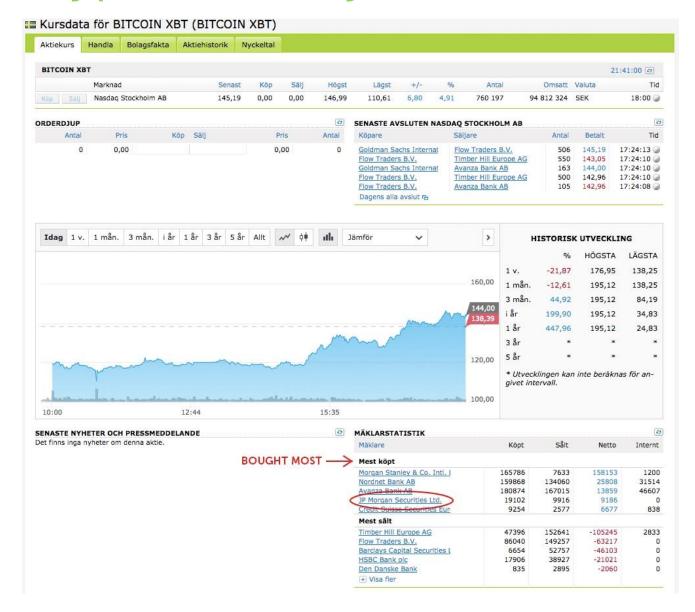
JPMorgan Chase CEO Jamie Dimon took a shot at bitcoin, saying the cryptocurrency "is a fraud."

https://www.youtube.com/watch?v=FaJUO-saPOs













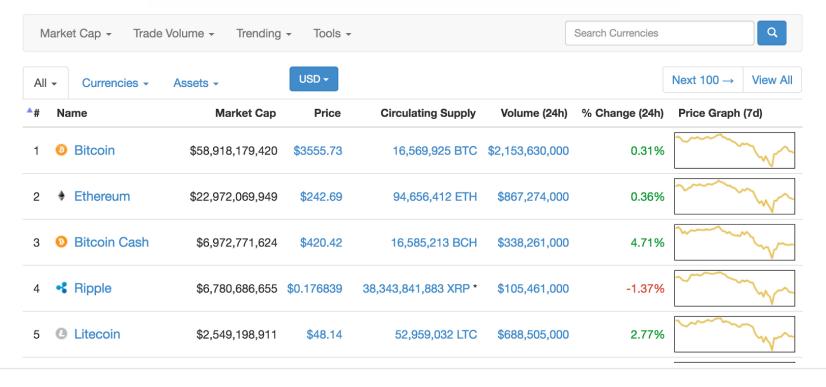
JP Morgan's chief executive, Jamie Dimon, might be getting into some trouble with Swedish financial authorities for market abuse when he called bitcoin a "fraud" last week.

Also read: Bitcoin Proponents Respond to JP Morgan Executive's Statements

THE STATE OF THE S

865 Currencies / 244 Assets / 5508 Markets Market Cap: \$121,564,797,361 / 24h Vol: \$5,385,085,872 / BTC Dominance: 48.5%

CryptoCurrency Market Capitalizations



51 🗷 ZCoin

\$35,828,232

\$11.79

3,038,995 XZC

\$10,495,100

4.49%

v V

















Yacoin Charts





Q&A

Questions and answers session