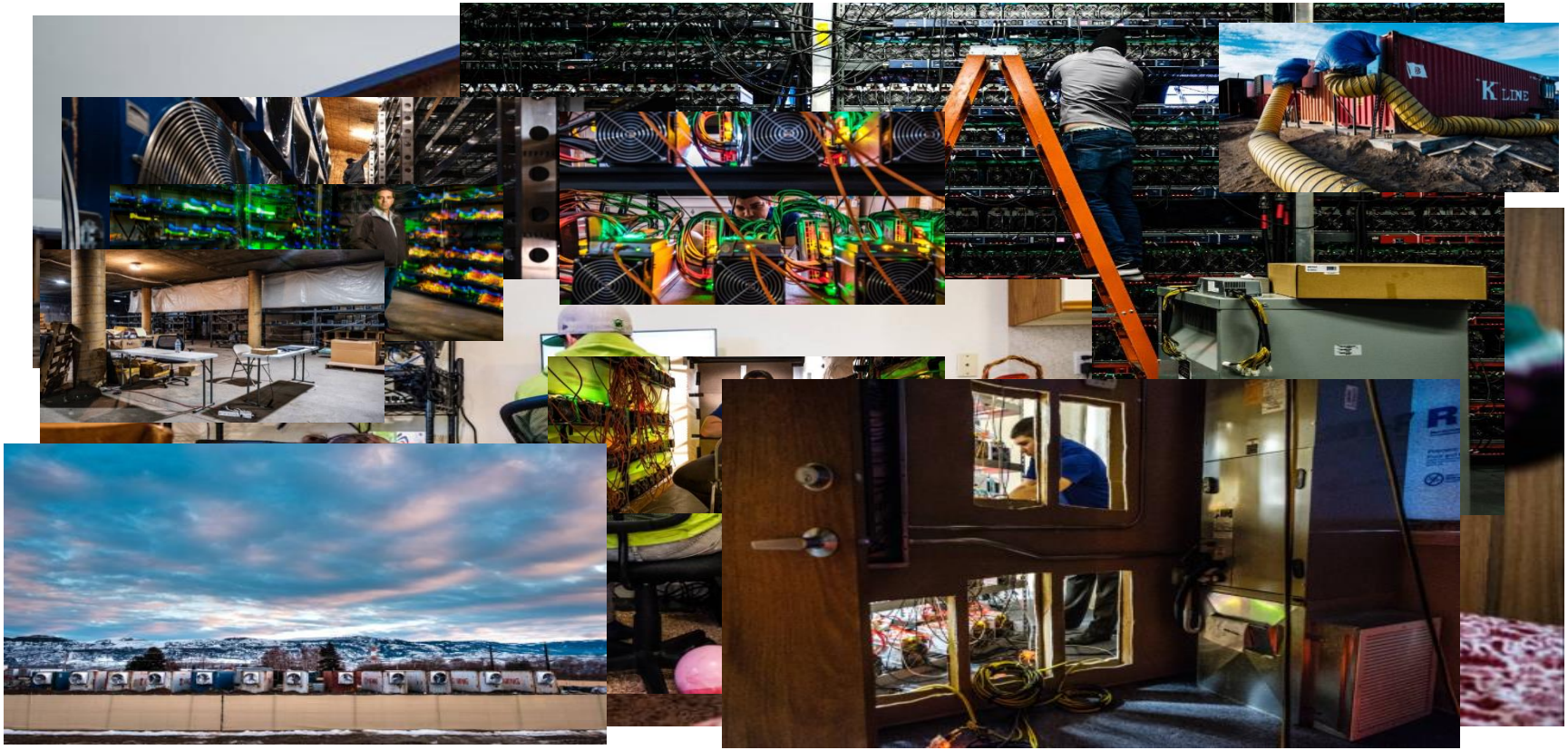
BITCOIN AND BLOCKCHAIN

Francesco Tonin
Bloomberg

Bloomberg

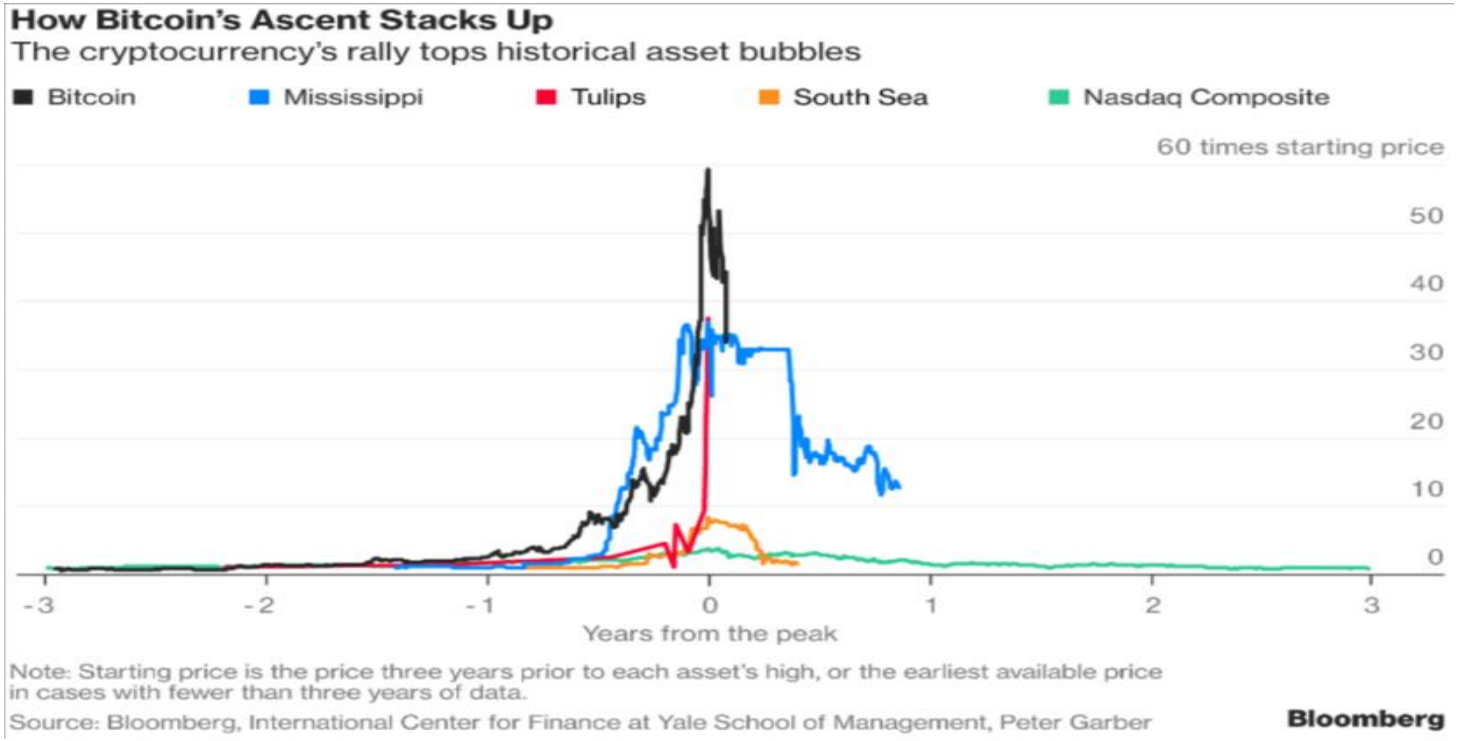
MAY // 8 // 2018

MINER'S LIFE



Reference: https://www.politico.com/interactives/2018/photo-essay-bitcoin-miners/

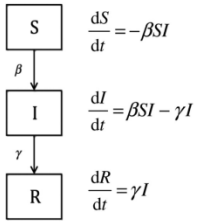
IF IT SMELLS LIKE A BUBBLE…

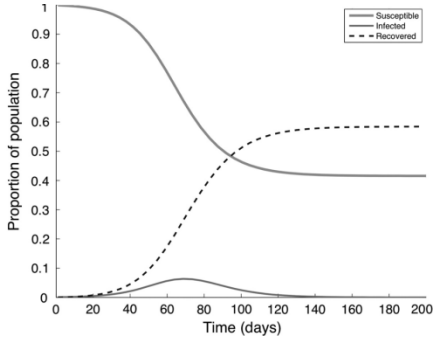


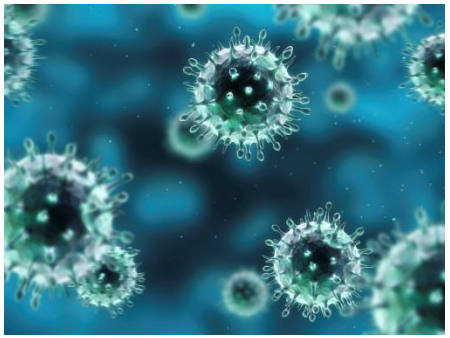
Reference: {NSN P2PEND6JIJUO <GO>}

INFECTIOUS DISEASE

Joseph Abate at Barclays has a very interesting interpretation of bitcoin in terms of pandemic deseases and memes theory.
“As more of the population become asset holders, the share of the population available to become new buyers -- the potential ‘host’ population -- falls, while the share of the population that are potential sellers (‘recoveries’) increases. Eventually, this leads to a plateauing of prices, and progressively, as random shocks to the larger supply population push up the ratio of sellers to buyers, prices begin to fall. That induces speculative selling pressure as price declines are projected forward exponentially.”
A similar dynamic plays out with infectious diseases when the so-called immunity threshold is reached, “the point at which a sufficient portion of the population becomes immune such that there are no more secondary infections,”







Reference: {NSN P6YMMN6KLVR7 <GO>} 10Apr18, and https://academic.oup.com/bmb/article/92/1/33/333536

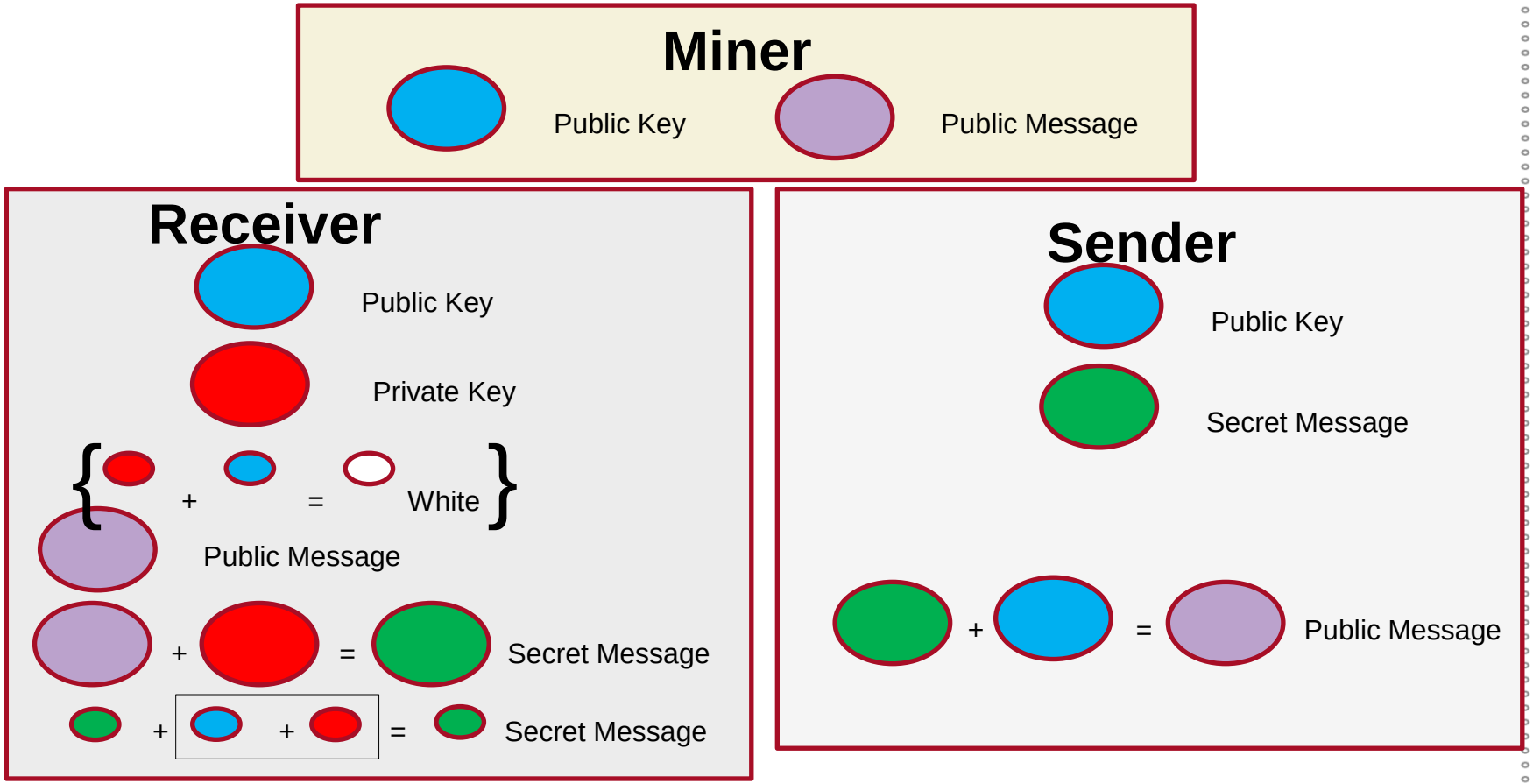
MARKET DATA AND SIZE

Cryptocurrencies market value: 800bio USD at peak, currently 400bio USD.
Transactions last 24hrs: 182,350

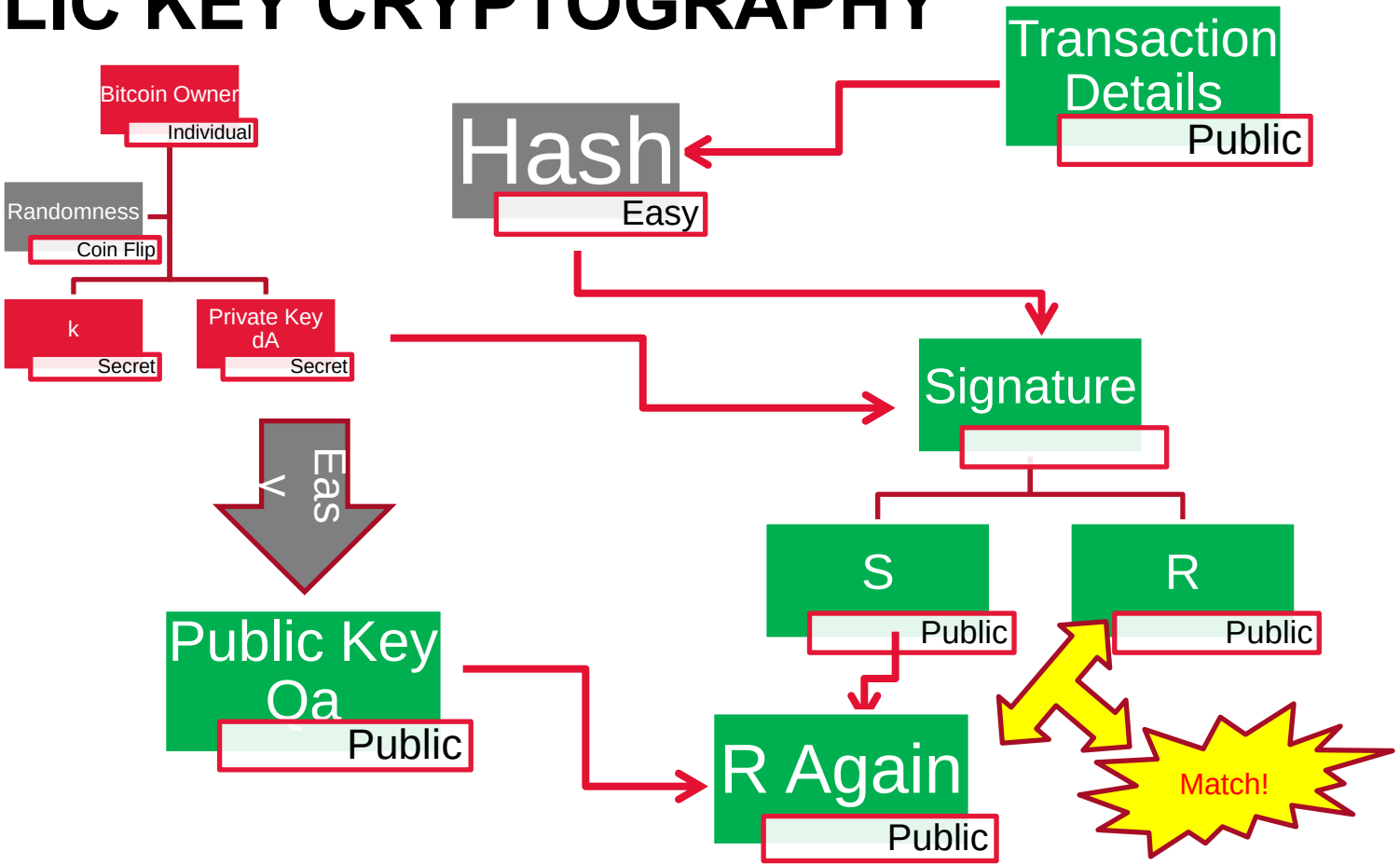
	Bitcoin	Ethereum	Ripple	Bitcoin Cash	Litecoin	Monero	Apple Inc.	S&P 500
Total	16mio	98mio	39bio	17mio	55mio	15mio	5bio	
Price	8k	500	0.6	860	131	195	170	
Market Cap	134bio	44bio	22bio	14bio	7bio	3bio	850bio	22tri
Transactions per Day	180k	580k	713k	78k	28k	4k	24mio	686mio
Avg. Transaction Value	6 btc	4.5 eth		6.65 bch	130k ltc			
Block Time	10min	15s		10m	2m	2m		
Active Addresses last 24hrs	400k	340k		41k	81k			
Tweets per Day	60k	18k	6k	2k	7k	1k	5k	

Reference: https://bitinfocharts.com

PUBLIC KEY CRYPTOGRAPHY



PUBLIC KEY CRYPTOGRAPHY



BABY EXAMPLE OF PUBLIC KEY

Locked: cannot figure out *d* even if you have *e*

Signature: choose e and d such that:

$$ed = 1\ mod(N)$$

e is the public key, *d* is the private key, *m* is the message. Owner computes the signature σ as:

$$\sigma = m^d\ mod(N)$$

Now *d* is still secred, and *e* and *m* were public anyways.

Now how do you prove that σ must have been created by somebody who has *e*? Verify that:

$$\sigma^e = m\ mod(N)$$

You will be able to verify it because:

$$\sigma^e = \left(m^d\right)^e = m^{de} = m\ mod(N)$$

So the probability that anybody can come up with σ such that without having d is close to zero (effectively zero).

HOW TO INVEST IN ICO'S

Here are a few options for buying bitcoin or ethereum with dollars:
Coinbase: market leader, easy to use, has mobile app
Gemini: A good option but more limiting
Bitpanda: never used myself
Coinmama: never used myself

These are top two favorite resources to learn about icos:
ICO drops (ICO drops)
Ico alert (ico alert)

Coin schedule (coin schedule)
ICO rating
ICO tracker
ICO list
Token market

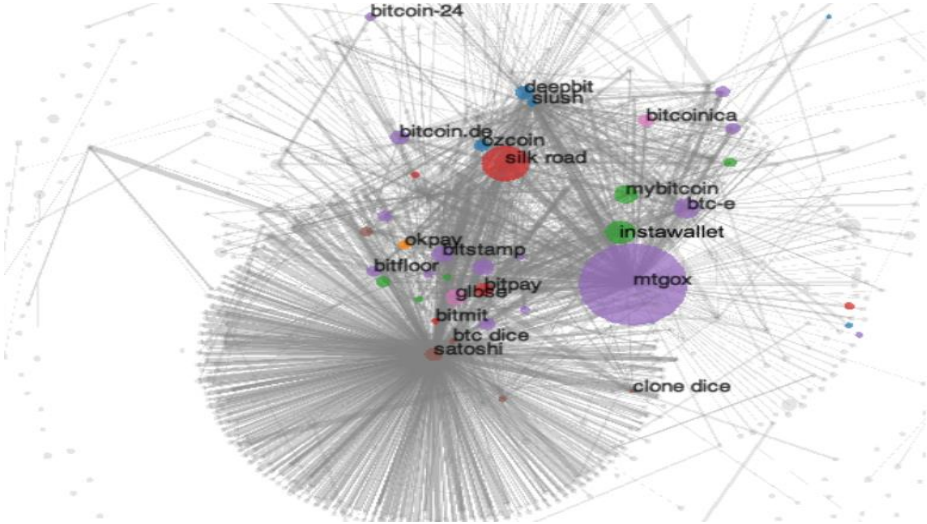
Reference: https://hackernoon.com/how-to-invest-in-icos-and-what-ive-learned-investing-in-five-icos-fc40f2a3b1fc

PERFORMANCE OF ICO'S

Cryptocurrency news site bitcoin.Com has surveyed last year's ico's and found that of 902 tracked by tokendata, 142 failed before raising funding, and another 276 failed after fundraising.

That's a 46% failure rate — but wait, there's more. Bitcoin.com found another 113 projects that it calls "semi-failed," because their teams have gone off the radar or their community has withered away. Add those, and the failure rate jumps to 59%. Bitcoin.com says the total funding of failed projects from 2017 was $233 million.

That's a lot of wasted money, though the failure rate might not seem outrageous for those familiar with startups. As many as 75% of all startups backed by traditional venture funding fail, and 30 to 40% of those take all of investors' capital with them. Out of all new companies started in the U.S., A little over 20% fail in their first year.



Reference: Http://fortune.Com/2018/02/25/cryptocurrency-ico-collapse/

CAVEAT EMPTOR

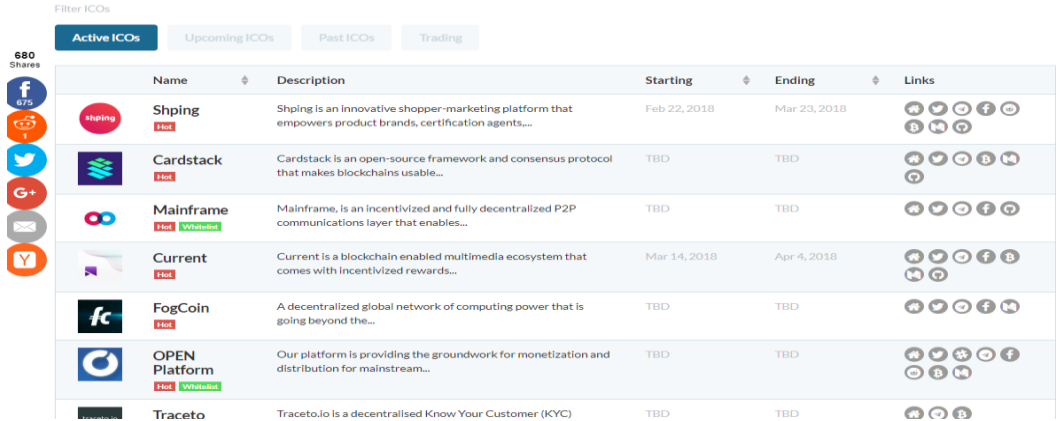
Coinbase knows who you are and collects personal information about you. Why does that matter? Recently, Coinbase was ordered to give the IRS data on its users trading more than $20K (read more). On the other hand, MyEtherWallet and Trust Wallet do not ask or retain any of your personal information.

Scammers are part of the ICO process. If you've participated in the ICO process, you know how crazy the telegram channel becomes. Scammers try to appear as admins or company representatives and lure you into sending coins to the wrong address. Some create admin-like posts in public chat in hopes that someone will get confused and send their funds to the wrong address.

ICOinsider

Telegram

ICO Hot List



Reference: https://hackernoon.com/how-to-invest-in-icos-and-what-ive-learned-investing-in-five-icos-fc40f2a3b1fc

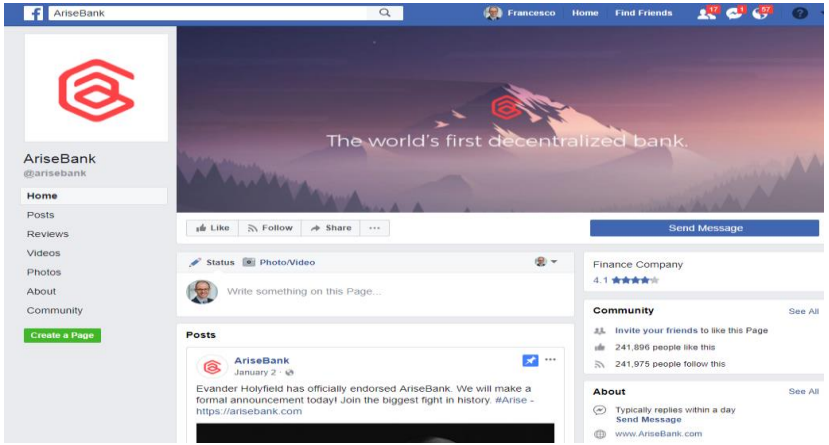
SCANDALS

February 2018:

texas’s top securities watchdog is halting cryptocurrency trading operation leadinvest, which allegedly targeted cryptocurrency trading newbies through a number of schemes.

Leadinvest allegedly touted having an all-star management team, implying its members included u.S. Supreme court justice ruth bader ginsburg, former U.S. Solicitors general, practicing attorneys with no relation to the company, and even photostock models, according to an emergency cease-and-desist order filed today.

Lead Invest Group
Property Development



Reference: {NSN P4RW6U3H0JK0 <GO>}

ANONYMITY AND BILL GATES

“Idioms of use" (e.g., transactions that spend coins from multiple inputs indicate that the inputs may have a common owner).
Corroborating public transaction data with known information on owners of certain addresses.
Additionally, bitcoin exchanges, where bitcoins are traded for traditional currencies, may be required by law to collect personal information.

Sarah Meiklejohn and colleagues created maps from that record that could help law enforcement find companies that hold identifying information for specific users.

An agency might, for example, follow the flow of bitcoins from an illegal transaction to a bitcoin exchange and then subpoena that company. “That would not be hard to do with the current patterns of how people are using things,” says Meiklejohn.

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy† Geoffrey M. Voelker Stefan Savage
University of California, San Diego George Mason University†

BSTRACT

coin is a purely online virtual currency, unbacked by either phys-
l commodities or sovereign obligation; instead, it relies on a
nbination of cryptographic protection and a peer-to-peer proto-

By far the most intriguing exception to this rule is Bitcoin. I
deployed in 2009, Bitcoin is an independent online monetary
tem that combines some of the features of cash and existing on
payment methods. Like cash, Bitcoin transactions do not explic

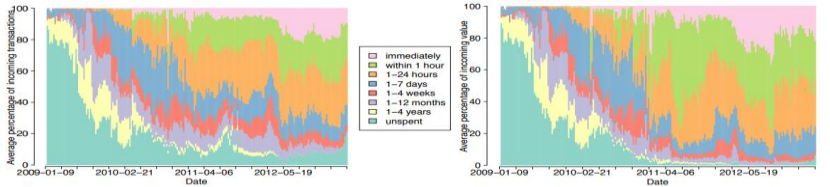


Figure 3: The trend, over time and averaged weekly, of how long public keys hold on to the bitcoins received. The plot on the left shows the percentage over all public keys, and the plot on the right shows the percentage over all value transacted. The values run bottom to top, from longest to spend (unspent as of now) to shortest to spend (spent within the same block).

It is difficult to invest much in bitcoin or realize gains made in the bitcoin economy, lawful or otherwise, without using an exchange.

The companies behind these exchanges handle millions of dollars’ worth of trades each month giving them a clear incentive to coöperate with authorities and abide by financial regulations.

Criminals tend to pay a lot of attention to the way they reclaim illegal bitcoins.

Reference: https://www.technologyreview.com/s/518816/mapping-the-bitcoin-economy-could-reveal-users-identities/

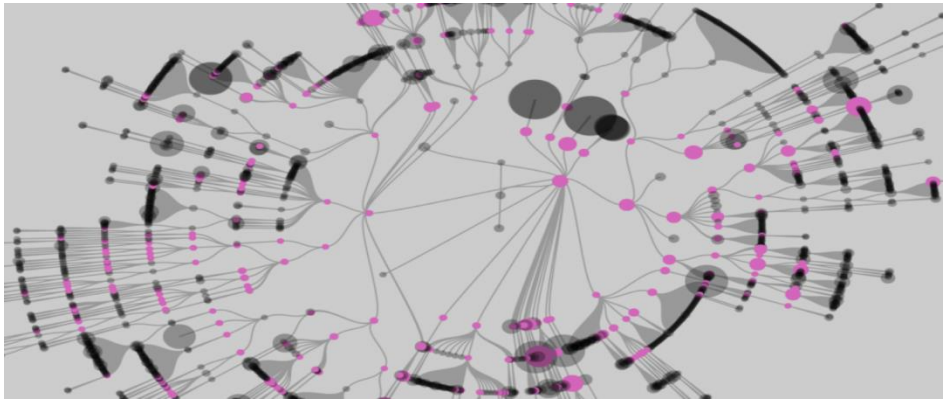
WANNACRY MONEY LAUNDERING

August 3, 2017, money was laundered, USD 140k

July 17, 2017, Patya/NotPetya ransomware money was laundered, USD 10k.

Could not use any exchange to withdraw money.

What is a bitcoin mixer?



Peer-to-peer tumblers appeared in an attempt to fix the disadvantages of the centralized model of tumbling. These services act as a place of meeting for bitcoin users, instead of taking bitcoins for mixing. Users arrange mixing by themselves. This model solves the problem of stealing, as there is no middleman. Such protocols as coin join, sharedcoin and coinswap allow few bitcoin-users to gather in order to form one bitcoin exchange transaction in several steps. When it is completely formed, the exchange of bitcoins between the participants begins. Apart from mixing server, none of the participants can know the connection between the incoming and outgoing addresses of coins. This operation can be carried out several times with different recipients to complicate transaction analysis

Reference: https://qz.com/1045270/wannacry-update-the-hackers-behind-ransomware-attack-finally-cashed-out-about-140000-in-bitcoin/

ANONYMITY

1) Publishing Your Name and Bitcoin Address Online: all the internet

2) Trading Bitcoins for National Currency on an Exchange: the exchange

3) Making purchases online using bitcoin: merchant or payment processor

4) Using a thin client or hosted wallet: server administrators

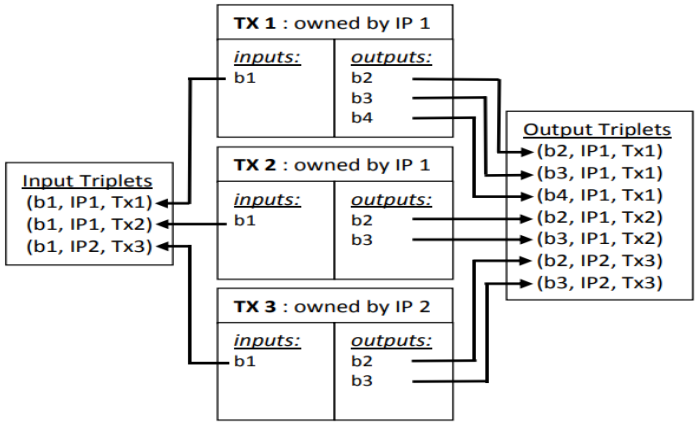
5) Using bitcoin without a VPN/Tor: your internet service provider

The Pennsylvania State University
The Graduate School

'343

AN ANALYSIS OF ANONYMITY IN BITCOIN USING P2P NETWORK TRAFFIC

A Thesis in
Computer Science and Engineering
by
Diana Koshy



Reference: https://99bitcoins.com/know-more-top-seven-ways-your-identity-can-be-linked-to-your-bitcoin-address/

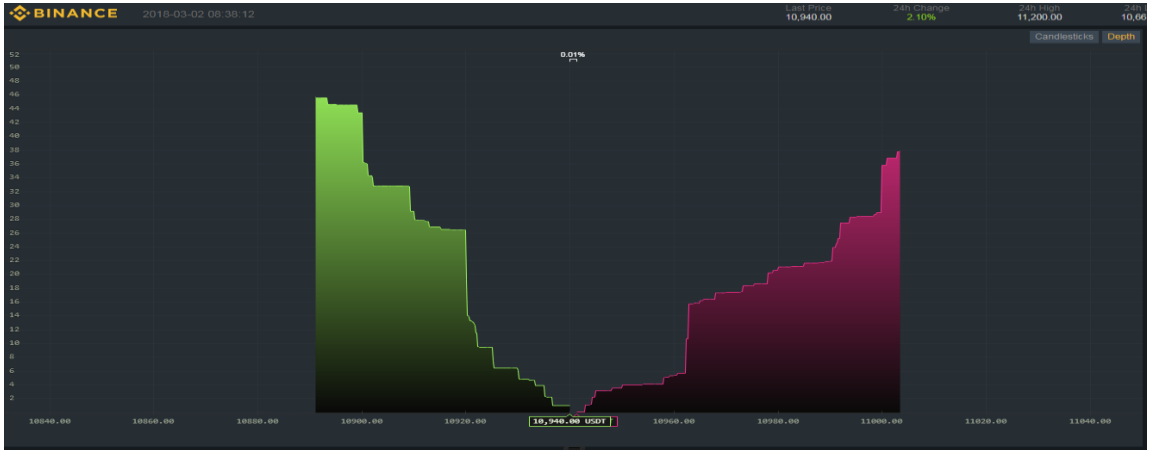
EXCHANGES

The top 10 are generating at least $40 million daily in fees and as much as $350 million, according to estimates compiled by Bloomberg using trading volume reported on data tracker CoinMarketCap.com and fee information on the exchanges' websites. Fees in the lowest range of the exchanges' scale were used for the calculations.

Reference: {NSN P54NWP6JIJVT <GO>}

ANALYTICS

Analytics on Bitcoin exchanges or web aggregation of information:



EXCHANGES MANIPULATION

Hacking of API keys allows for hacking of trade activity but no withdrawal of funds

A large order on VIA/BTC increased the price of VIA sevenfold

Users reported unauthorized buy trades on VIA

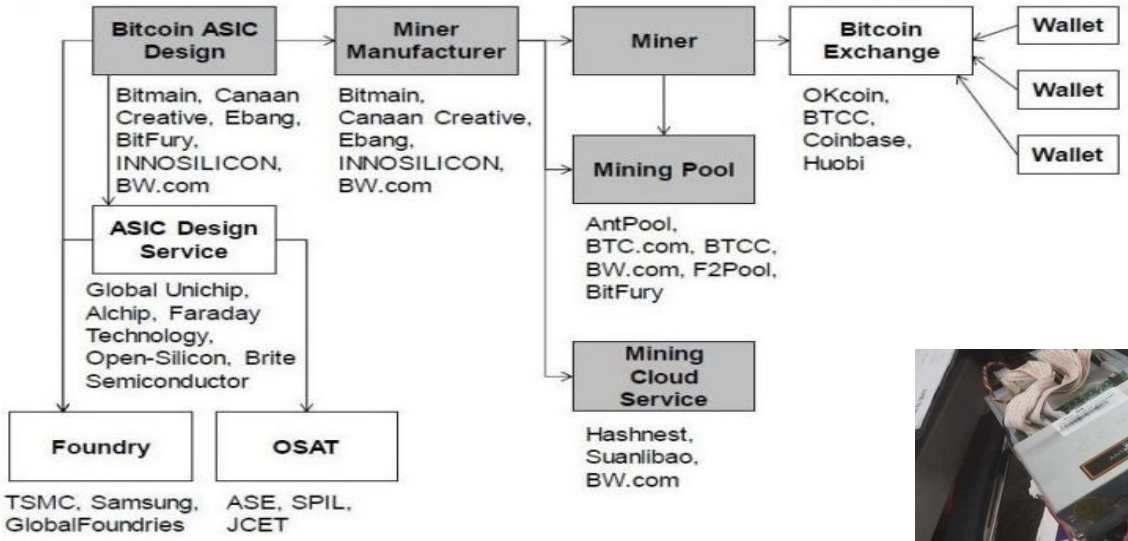
VIA/BTC Price Chart

Reference: {NSN P58I9ZAIBMDX <GO>}

HIDDEN BITCOIN PROFITS

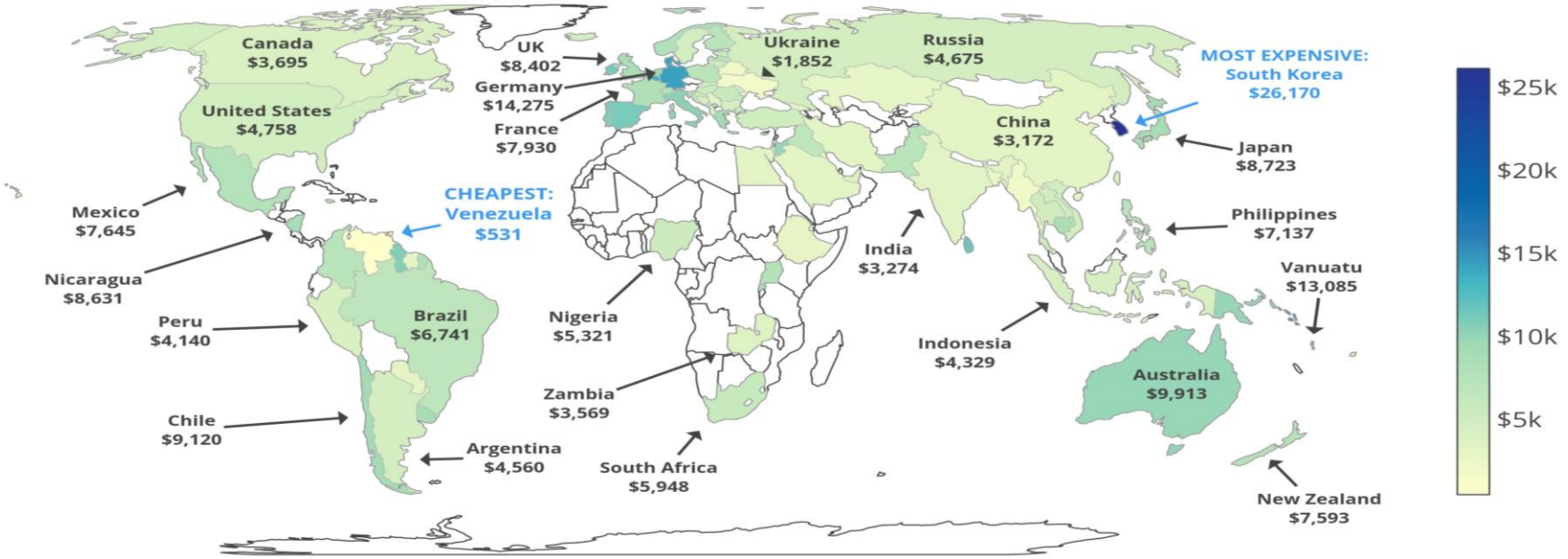
BITCOIN MINING GIANT BITMAIN RAKED IN $3 TO 4 BILLION IN PROFITS LAST YEAR

NVIDIA profit was 3 bio last year. Thanks to their dominance on all fronts, Bernstein estimates that Bitmain holds claim to somewhere between 70 percent and 80 percent of Bitcoin mining's total market share.



Reference: {NSN P4Q2C4AIBMDE <GO>}

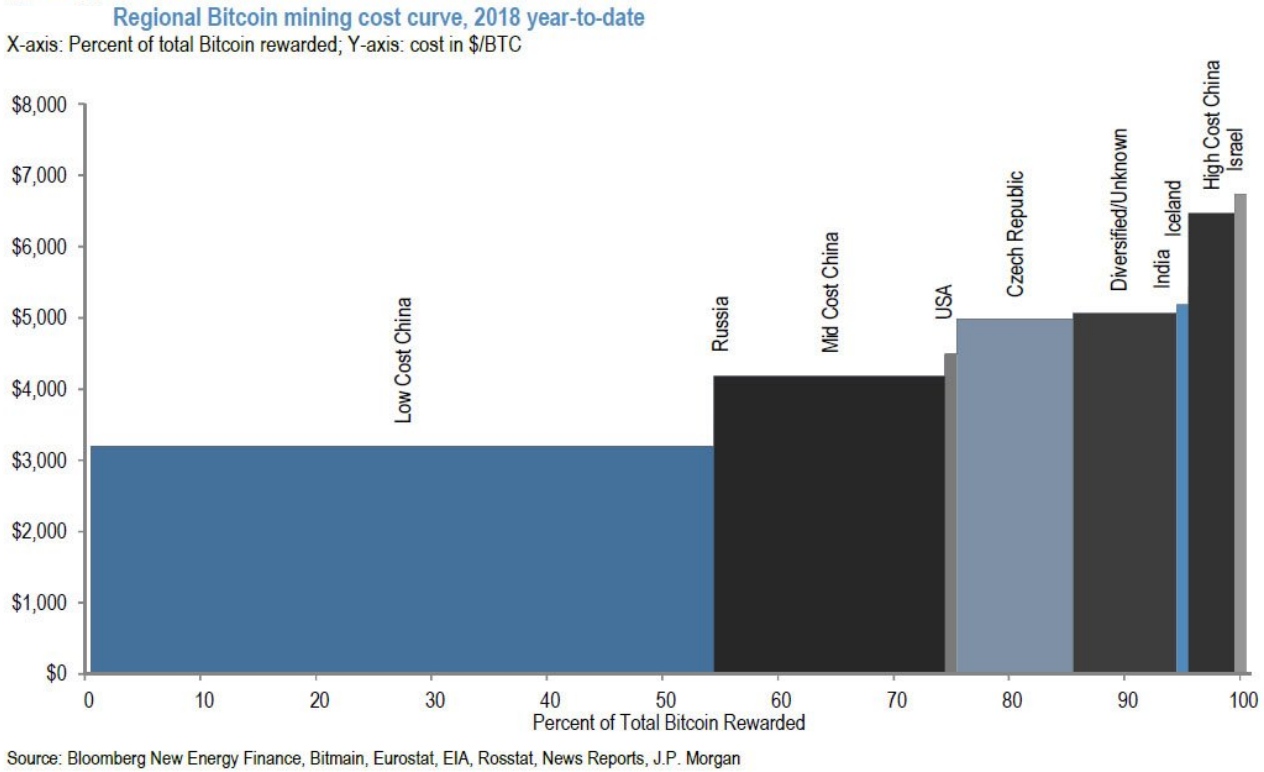
THE COST OF MINING ONE BITCOIN



Reference: http://bitcoinist.com/japan-mining-solar-energy-competitiveness/

http://bitcoinist.com/mapped-cheapest-expensive-countries-mine-bitcoin-electricity-cost/

THE COST OF MINING ONE BITCOIN



Reference:https://twitter.com/zerohedge/status/982259754285252613/photo/1

CRYPTO ELECTIONS

Agora
Bringing our voting systems into the 21st century

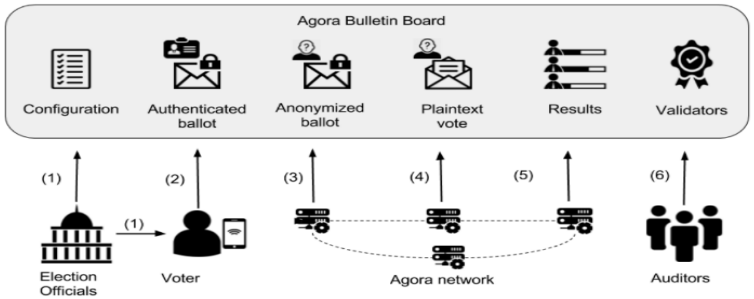
Startup Agora carried out the first instance of an official election where part of the votes were certified via blockchain technology on March 7.

The election was held in Sierra Leone's Western District, where Freetown, the capital, is located.

The ballots were still paper, but after the vote each of them was logged into a specialized blockchain. This was only accessible to election officials, but this is not necessary, as security would still be guaranteed even In case the whole blockchain is public.

Opposition leader Julius Maada Bio of the Sierra Leone People's Party led with 43.3 percent of the vote in the first round of elections but failed to secure a majority vote needed to win, according to the electoral commission.

The run-off was delayed several days due to a complaint of fraud lodged by a member of the APC. A court injunction was lifted a day before the polls were due to take place last tuesday, forcing the elections commission to push back the vote.



Reference: {NSN P5K2FIBUJSBC <GO>}, {NSN P6PL2I3H0 <GO>}

STATE OWNED CRYPTOS

The newest cryptocurrency is the invention of Venezuelan president Nicolás Maduro. The "petro," as the cryptocurrency is known, was launched this week as a very creative hail mary by a struggling autocrat.

The website for the cryptocurrency claims that in its first issue, opened for trading on Feb. 20, it made available 100 million tokens, each selling for about $60, a figure that is close to the price of a barrel of oil. Each petro is supposedly backed by a barrel of oil, though analysts are not sure what this means in practice. Maduro values this issuance at $6 billion: $60 for each token for 100 million tokens.

Can only buy using USD. Inspection of the blockchain reveals about half the claimed amount of petros.

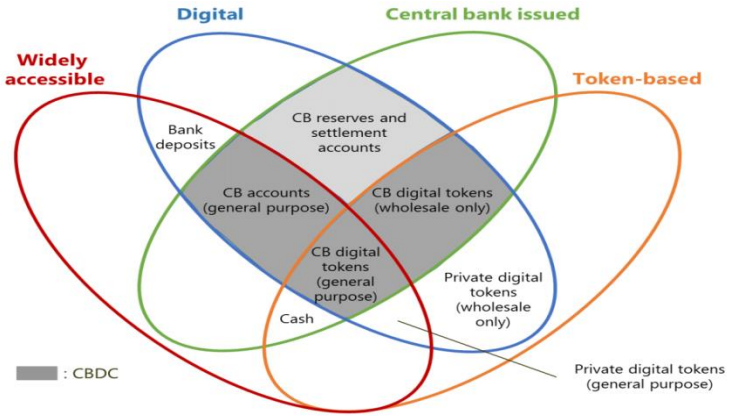
nem
a new economy starts with you.

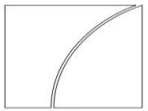
Reference: {Nsn p4rjy33hbs3l <go>}

CENTRAL BANKS CRYPTOS

	Existing central bank money		Central bank digital currencies		
	Cash	Reserves and settlement balances	General purpose token	General purpose accounts	Wholesale only token
24/7 availability	✓	×	✓	(✓)	(✓)
Anonymity vis-à-vis central bank	✓	×	(✓)	×	(✓)
Peer-to-peer transfer	✓	×	(✓)	×	(✓)
Interest-bearing	×	(✓)	(✓)	(✓)	(✓)
Limits or caps	×	×	(✓)	(✓)	(✓)

✓ = existing or likely feature, (✓) = possible feature, × = not typical or possible feature.





Committee on Payments and Market Infrastructures

Markets Committee

Central bank digital currencies

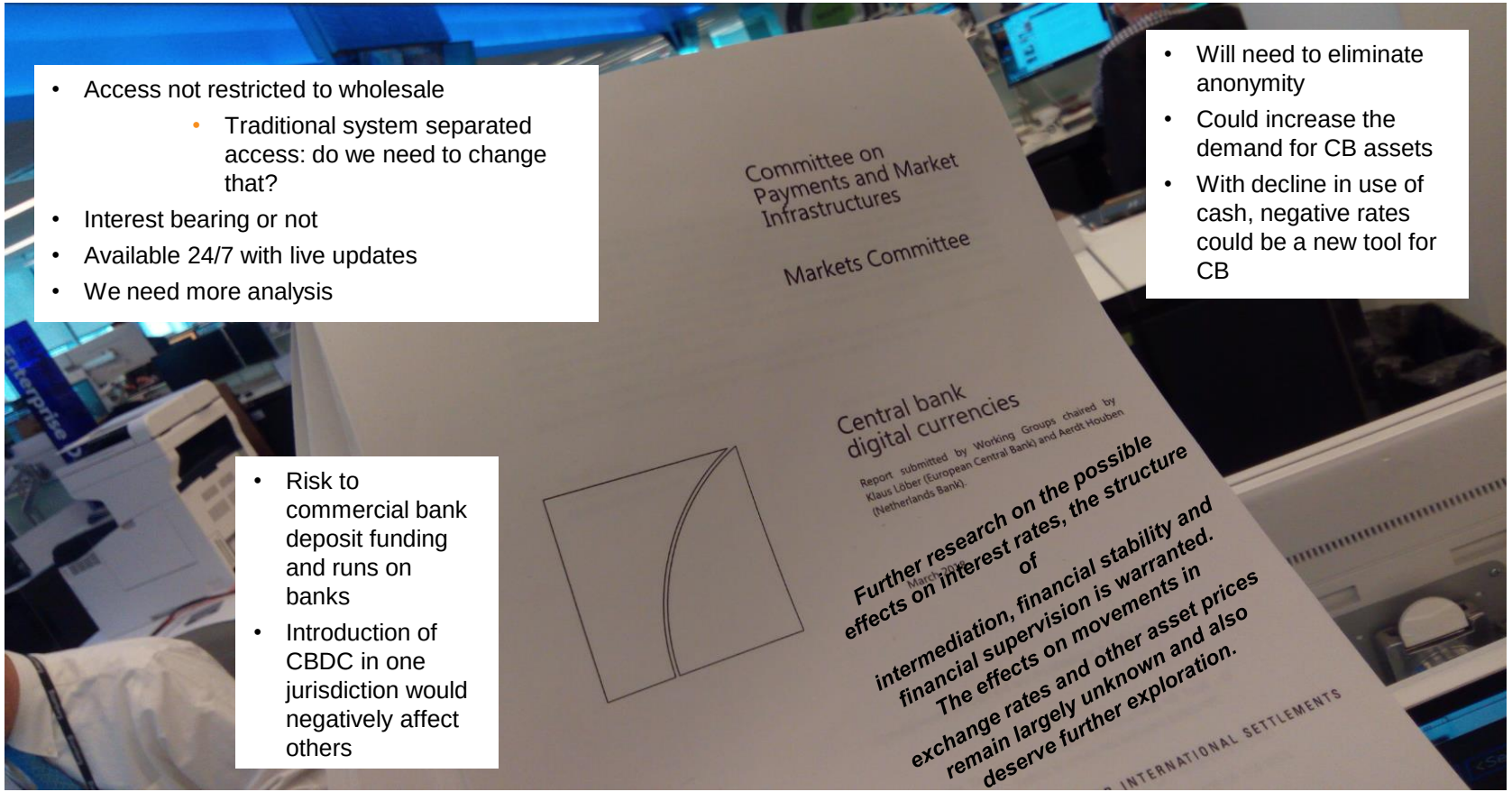
Report submitted by Working Groups chaired by Klaus Löber (European Central Bank) and Aerdt Houben (Netherlands Bank).

March 2018

BANK FOR INTERNATIONAL SETTLEMENTS

Reference: https://www.bis.org/cpmi/publ/d174.pdf

CENTRAL BANKS CRYPTOS



- Access not restricted to wholesale
  - Traditional system separated access: do we need to change that?
- Interest bearing or not
- Available 24/7 with live updates
- We need more analysis

- Will need to eliminate anonymity
- Could increase the demand for CB assets
- With decline in use of cash, negative rates could be a new tool for CB

- Risk to commercial bank deposit funding and runs on banks
- Introduction of CBDC in one jurisdiction would negatively affect others

FSB LETTER TO G20 IN BUENOS AIRES

FSB FINANCIAL STABILITY BOARD

THE CHAIR

13 March 2018

To G20 Finance Ministers and Central Bank Governors

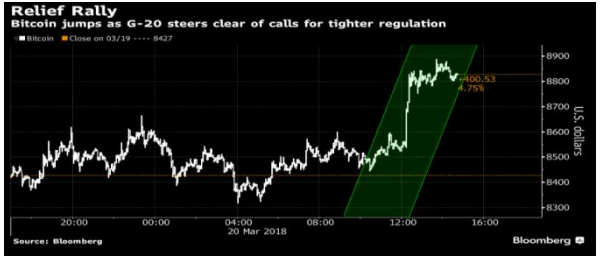
G20 Finance Ministers and Central Bank Governors are meeting against a backdrop of strong and balanced global growth. This momentum is underpinned by a resilient global financial system that is the product of determined efforts by the G20 and FSB over the past decade.

banking and are transforming the remaining activity into resilient market-based finance. Reforms to over-the-counter derivative markets are replacing a complex and dangerous web of exposures with a more transparent and robust system that better serves the real economy.

Crypto-assets

Responding to the concerns of members, the FSB has undertaken a review of the financial stability risks posed by the rapid growth of crypto-assets.

The FSB's initial assessment is that crypto-assets do not pose risks to global financial stability at this time. This is in part because they are small relative to the financial system. Even at their recent peak, their combined global market value was less than 1% of global GDP. In comparison, just prior to the global financial crisis, the notional value of credit default swaps was 100% of



G20 ARGENTINA 2018

BUILDING CONSENSUS FOR FAIR AND SUSTAINABLE DEVELOPMENT

Reference: https://cointelegraph.com/news/dont-read-too-much-into-the-fsbs-letter-to-the-g20-on-bitcoin-expert-take

GENERAL DAPA PROTECTION REGULATION

Issues relevant to the regulation:

Encryption

Immutability

Transparency

Public vs. Permissioned

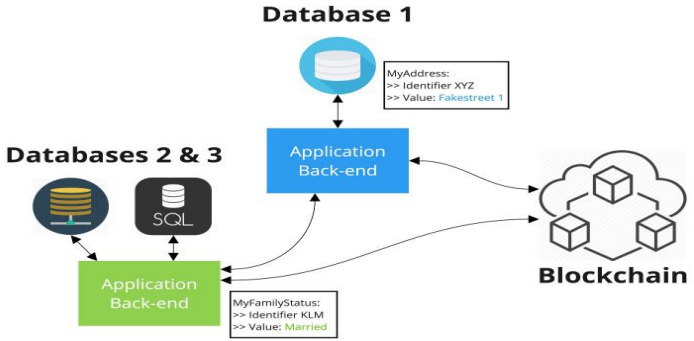
CRUD: create read update delete

Create retrieve append burn: through away the keys

Personal data is NOT to leave the EU

Right to be forgotten

No definition of “erase”: is throwing away the private keys equal to “erase” the data?



So personal data CANNOT be stored on the blockchain, but a hash of the data could, which would guarantee that the data is authentic, and a data request could be honored by a link and password, but the data itself is not on the blockchain

References: https://www.ccn.com/gdpr-a-game-changer-is-coming-for-cryptocurrency/, GDPR FAQ: https://www.eugdpr.org/gdpr-faqs.html, https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047, Full text of regulation: https://gdpr-info.eu/:

RIPPLE PARTNERSHIPS

Moneygram will pilot the use of XRP, the native digital asset of the XRP ledger, in payment flows through xrapid, ripple's solution for on-demand liquidity. XRP remains the most efficient digital asset for payments with transaction fees at just fractions of a penny, compared to bitcoin fees of about **$30** per transaction. Similarly, the average transaction time for XRP is 2-3 seconds with other top digital assets ranging from 15 minutes to an hour.

Sbi virtual currencies (sbi vc) is looking to join the xrapid ecosystem — ripple's enterprise-grade solution — to help institutions source liquidity for cross-border payments between japan and the rest of the world. Ripple will eventually integrate SBI vc's apis so that xrapid users — payment providers and banks who are transferring money into and out of japan — can convert XRP to JPY and JPY to XRP instantly through SBI VC.

On this day ripple partnered with two more financial services in its tight race to establish itself as a crypto of choice for the establishment. The two companies are **IDT** and **mercury FX** which resolved to utilize ripple (XRP) currency. This currency runs exclusively on the xrapid-service which will facilitate sending of cash anywhere in the world at an extremely low cost.

Lianlian International, one of the leading chinese payment providers made a groundbreaking move to join ripplenet. The company plans to utilize xcurrent, which is ripple's settlement solution. It powers cross-border transactions between china and europe as well as the US.

Ripple and **Saudi Arabian Monetary Authority** (sama) embarked on a pilot program aimed as saudi banks. The aim is to assist banking institutions improve their payment systems via the use of xcurrent. The authority intends to use xcurrent for the instant settlements of payments into and out of the country at minimal cost and more transparency.

References: https://www.bloomberg.com/news/articles/2018-01-25/ripple-wants-xrp-to-be-bitcoin-for-banks-if-only-the-banks-wanted-it
Https://cryptorecorder.Com/2018/03/01/ripple-xrp-2018-5-major-partnerships-and-announcements/

RIPPLE PARTNERSHIPS

76bio USD a day in payments. That is double the US GDP produced each day.

Ripple has signed a lot of banks onto its network and sold equity stakes in itself to Standard Chartered plc and Banco Santander sa. Influential names from Wall Street such as Zoe Cruz, the onetime co-president for institutional securities and wealth management at Morgan Stanley, joined Ripple's board. Of the more than 100 companies, though, Garlinghouse would specify the transaction volume of only one, Stockholm-based Skandinaviska Enskilda Banken AB, which he said moved just shy of $1 billion in payments over Ripplenet. Even investors Standard Chartered and Santander haven't taken the plunge and are only testing the technology.

In November 2017, Standard Chartered started a program to send payments between Singapore and India for its corporate clients. Even though neither bank plans to use XRP in these projects, both are optimistic about Ripple's technology.

Nor is Swift taking the challenge lying down. It recently rolled out its own major upgrade called Global Payments Innovation, or GPI. It allows banks' corporate customers to make payments in a couple of hours and to track transactions on their journeys the same way Fedex Corp. Customers can.

Recipients receive same-day access to payments rather than waiting several days for funds to clear.

Fees should be predictable and transparent, so businesses know in advance how much wire transfers will cost.

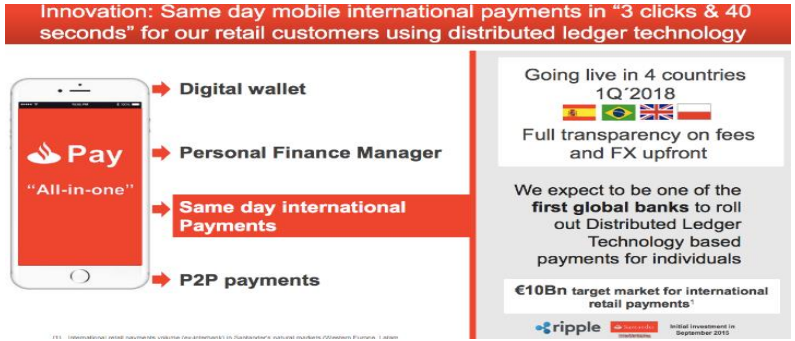
Banks can use a new cloud-based service to track each payment from end-to-end as it passes through intermediary banks and ultimately reaches the recipient's account. Payers receive confirmation that the recipient's account has been credited.

Up to 140 characters of remittance information is transferred unaltered to recipients, helping them reconcile payments.[3] [120] Banks representing 75% of current SWIFT payments, 2 mio messages, 24 banks live and using the service, 24 hour cycle time, API allows to track in real time.

SANTANDER AND RIPPLE

For now, the focus lies on Spain, Brazil, The UK, and Poland. This launch will occur at some point in the next three months. No further specifics have been announced just yet. We do know all transactions will be settled within 24 hours or less. It is a big step up from how cross-border transactions are handled as of right now.

More importantly, this new solution offers unprecedented transparency. Users can figure out the exact transaction cost beforehand, which is rather impressive. For now, we have to wait and see if this new solution will make use of XRP as well. There is no official indication that will effectively be the case, but the details are scarce. Assuming the project is successful, the appeal of ripple will only continue to increase.



Reference:{NSN P63WPJAIBMDQ <GO>}

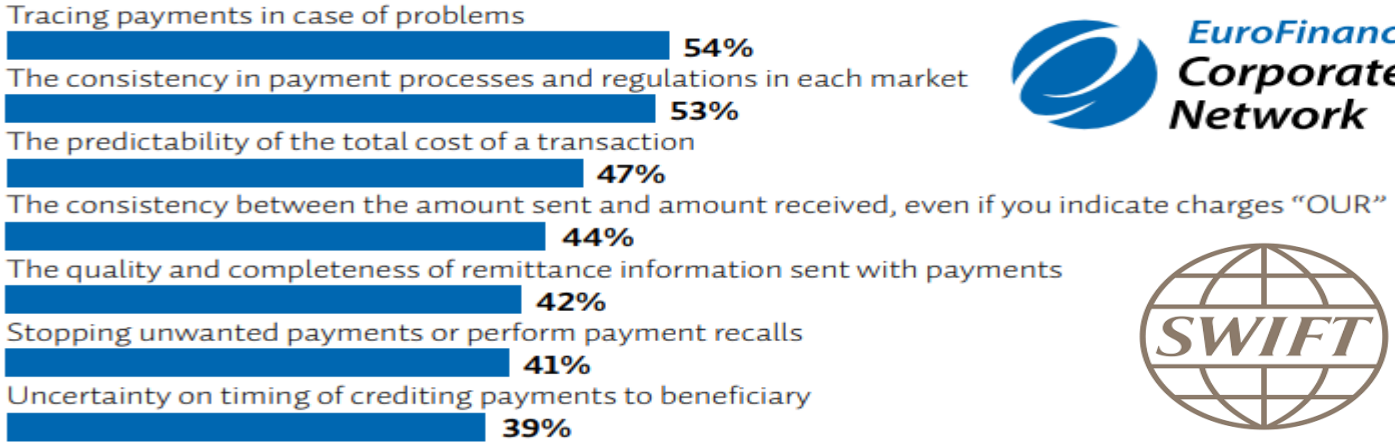
SANTANDER AND RIPPLE

Santander has launched a foreign exchange service that uses blockchain technology to make same-day international money transfers.

The service, called Santander One Pay FX, uses tech developed by blockchain firm Ripple. Santander said it is the first cross-border payments service using blockchain to be made by a bank.

Reference: https://www.cnbc.com/2018/04/12/santander-launches-blockchain-based-foreign-exchange-using-ripple-tech.html?mod=djemDailyShot&mod=djemDailyShot

PAYMENTS: STATE OF THE UNION



EuroFinance Corporate Treasury Network

SWIFT

In parallel, SWIFT is exploring the potential use of blockchain technology in the cross-border payments process. Over 30 GPI banks have been running a proof of concept (poc) to test whether a swift-developed application using distributed ledger technology (DLT) can be used to reconcile nostro accounts in real-time and help to optimise global liquidity. Preliminary results will be shared at Sibos in toronto whilst the poc is set to finish later in November 2017.

Al Baraka Bank, Asociación Popular De Ahorros Y Préstamos, Axis Bank, Banco De Chile, Banco De Crédito Del Perú, Banco De Galicia, Banco De Reservas De La República Dominicana, Banco Del Pacifico, Banco Inbursa, Banco Sabadell, Bangkok Bank, Bank Al Etihad, Bank Of Georgia, Bank Of Jiangsu, Bank Of Montreal, Bank Of Ningbo, Bank Of Shanghai, Bank Of Tokyo-mitsubishi UFJ, Bank Of Zhengzhou, Bidvest Bank, Budapest Bank, Caixabank, Grupo Cooperativo Cajamar, Canadian Imperial Bank Of Commerce, Central Africa Building Society, China Zheshang Bank, Chong Hing Bank, Crédit Agricole, Credit Suisse, CTBC Bank, E.SUN Commercial Bank, Ecobank, GCB Bank, HELABA Landesbank Hessen-thueringen, ICICI Bank, Ipagoo, Kapital Bank Azerbaijan, Kasikorn Bank, National Commercial Bank, Powszechna Kasa Oszczednosci, Promsvyazbank PJSC, Scotiabank, Shanghai Rural Commercial Bank, Skandinaviska Enskilda Banken, Turkiye Garanti Bankasi, UBS Group, United Overseas Bank, Vietcombank, VTB Bank And Yinzhou Bank.

BANKING PROGRESS

“Going from that PoC in 2016, we’re at the tipping point of getting our customers involved in live transactions in the coming weeks and months. The technology has come a long way, we’re much more comfortable with its security and scalability.”

HSBC is not alone in this field, with today’s news following an announcement coming from Taiwan’s central bank chief revealing the bank will explore blockchain applications in its operations including payments. The development is occurring around the world – last year fifteen of India’s largest banks formed a consortium to oversee the introduction of an inter-bank blockchain, with the goal of integrating blockchain alongside existing infrastructure and technologies.

Blockchain is integrating into financial systems at a rapid pace, and one of the main players has emerged in the form of the virtual currency Ripple. Earlier this month news broke that Brazil and Latin America’s largest bank would use the virtual currency to streamline its cross-border payments system, joining a broad range of countries planning to use the protocol.

HSBC

Reference:{NSN P4XGPWAIBMDN <GO>}

APPLICATIONS: BUILDING A TOKEN IN TEN MINUTES

You can practice issuing your own security token. It takes about ten minutes.

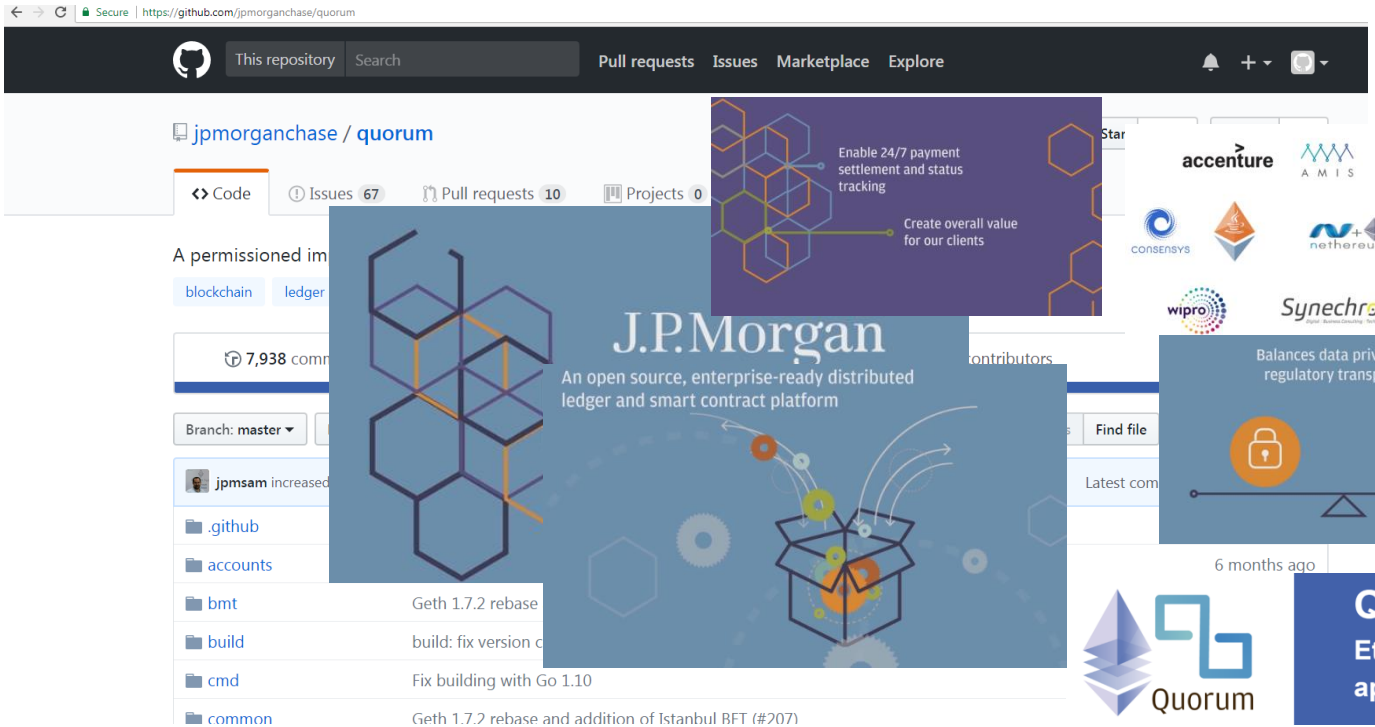
MATADOR ADVISORS

LAUNCHING TOKENS FOR THE MASSES

Reference: https://www.polymath.network/wizard

JPMORGAN QUORUM

- This is a network for payments, which will maintain confidentiality and will be based on P2P architecture



Reference: https://www.jpmorgan.com/country/US/EN/Quorum

APPLICATIONS: BUILDING A PLANE

Several parties have to access information on an asset gathered over years and has to be safe from manipulation. All events in the lifecycle of the airplane like owner change, planned and unplanned inspections, numbers of flights and covered distance should be saved and trackable.

A smart contract on a public blockchain is the perfect way to gather and store information over a long period of time, and guarantee availability, immutability, and independence from any intermediary.

The involved companies can all rely on the technical interfaces provided with the “Asset Lifecycle” Template. The integration into individual systems of each party can be established by defining suitable workflows based on the template by using the Unibright Workflow Designer. The Unibright conformant smart contracts can be published into a public blockchain by the Unibright Contract Lifecycle Manager and are connected to individual IT systems by the Unibright Connector. The current state of the process can be monitored any time with the Unibright Explorer and can be presented to the public.

Reference: https://www.newsbtc.com/2018/03/05/unibright-integrate-blockchain-business/

APPLICATIONS: PROCUREMENT

A product manager for a casual wear company is responsible to develop a design process of a new hoodie, and coordinate all departments and their respective approval on the ongoing design process. She checks the current approval state in the company's ERP system and sees that Tom from the Marketing department just gave his final ok on the marketing materials. She sees that the next approval should come from buying department submitting the prime costs.

Anna from the buying department has to keep track of all offers of the different suppliers who would be able to produce the new hoodie. She has to get back to the other departments for detailed questions and only communicate by phone or email, as the suppliers are not integrated into the process due to security reasons.

The existing approval process works fine, except the supplier part. Anna has to do all the approval work manually, which is time consuming and error-prone. The blockchain can act as a state-machine: secure, reliable and deterministic. The current state of the approval process can be accumulated in a central smart contract which holds the control flow and implicitly decides on the final approval state.

Unibright's "Multi-Party-Approval" Template offers a use case related predefined integration workflow for approval processes which can be customized. Steve from the IT department set up a private blockchain between all suppliers and the company. He designed the integration process visually with the Unibright Workflow Designer. The Unibright Contract Lifecycle Manager generated the needed Smart Contracts. The Unibright Connector integrates the existing ERP by automatically generated Smart Adapters.

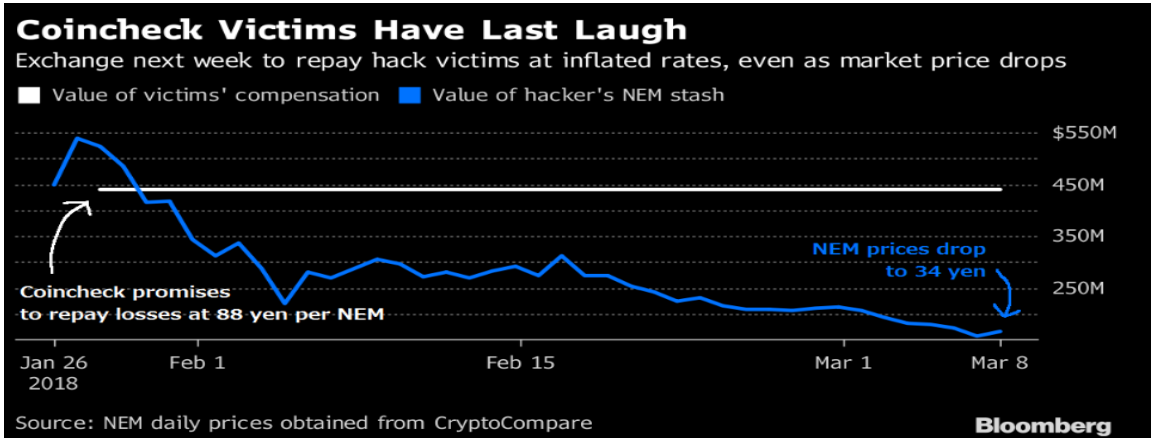
Reference: https://www.newsbtc.com/2018/03/05/unibright-integrate-blockchain-business/

PARADOXES: GAINS BY HACK

For victims of the $500 million heist at Japanese cryptocurrency exchange Coincheck Inc., getting robbed may have been a blessing in disguise.

The 260,000 traders who lost money in the theft will be reimbursed by Coincheck at a rate of about 88 yen (84 U.S. cents) for each NEM coin that was stolen from their accounts, Chief Operating Officer Yusuke Otsuka said on Thursday, bringing the total payout to about $440 million.

That's $262 million higher than the current market value of the stolen coins, which have slumped since the theft in January amid a broad retreat in cryptocurrencies. Coincheck said it's using company funds to reimburse victims and will start the payouts as soon as next week.



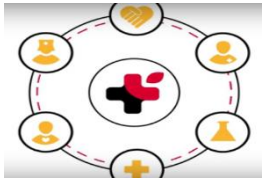
Reference: {NSN P59SH16K50XS <GO>}

APPLICATIONS: MEDICAL RECORDS

Patientory is already using blockchain technology to permit its users to store and access health data and securely message one another. In May, the company also released its own cryptocurrency, PTOY, in an initial coin offering (ICO) that netted Patientory $7.2 million in three days.

“Claims can sometimes take 30–90 days to process. That time is shortened by the use of digital currencies.”

By providing a secure layer upon which users can message one another, access their electronic health records, and send and receive money for medical services, Patientory is using the blockchain to achieve interoperability between traditionally siloed components of the healthcare system like patient communication, data storage, and payment.



BLOCKCYPHER

patientoryinc

Reference: {NSN P59SH16K50XS <GO>}, https://healthtransformer.co/patientory-takes-another-big-step-towards-interoperability-2d1741d39ca

APPLICATIONS: TRADE FINANCE

GTR Global Trade Review

Barclays announced in September 2016 that it has completed the world's first tradefinance transaction using blockchain payment technology, alongside a startup called Wave, which the british bank first backed about a year ago.

The transaction used blockchain technology to transfer documents between Ireland's Ornua cooperative, the former Irish Dairy Board and the owner of Kerry Gold Butter, wholesaler Seychelles Trading co. and barclays.

The transaction involved Seychelles using a Barclays letter of credit to buy goods from Ornua. Wave's blockchain technology enabled trade finance documents to be sent backwards and forwards between parties, digitally, circumventing what can be a lengthy process requiring multiple transfers of physical documents using couriers.

Barclays and Wave are seeking to take blockchain mainstream in trade finance and are keen to enlist other banks and trade clients in order to do this. The Barclays and Wave teams say that, with the right development, the technology can reduce the time it takes to complete a trade finance transaction from days, to hours. In the Barclays pilot, the parties were able to execute an export letter of credit in just four hours – something that generally takes seven to 10 days.

The bank was one of the first U.K. Institutions to partner with a crypto currency firm when it provided underlying currency accounts to users of Circle, a social payments app for crypto currencies, at a time when the mainstream banking industry had shunned the idea of bitcoin and other crypto currencies.

BARCLAYS

Barclays Accelerator

techstars

WAVE

PILGRIMS CHOICE

Ornua

THE HOME OF IRISH DAIRY

Kerrygold Irish Cream Liqueur

Beo Milk

Shannon Gold

Dubliner 100% Natural Cheese

CIRCLE

STC Seychelles Trading Company Ltd.

Values your trust

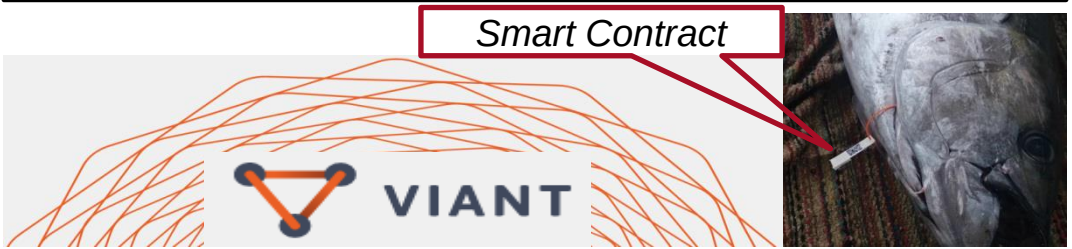
Reference: {NSN OD6L0OBUV0UC <GO>}

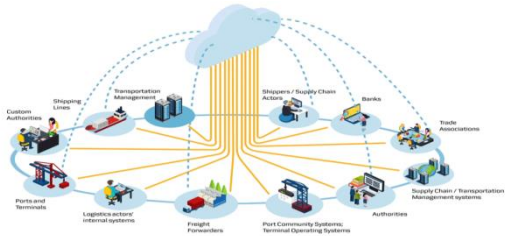
APPLICATIONS: TRADE FINANCE

Avocado shipments take 200 interactions with 30 parties to complete.
A full container ship can include hundreds of thousands of transactions.
Bills of landing, packing lists, letters of credit,m insurance policies, orders, invoices, sanitary certificates, certificates of origin…

Twenty percent of shipping cost is paperwork.

Full digitisation could raise Asia-Pacific's exports by about 250bio a year, according to the World Economic Forum.





Reference: https://media.economist.com/news/finance-and-economics/21739159-administrative-obstacles-loom-larger-technological-ones-digitisation

APPLICATIONS: TRADE FINANCE

In keeping with ibm's commitment to open source, the solution is run from the IBM blockchain platform on hyperledger fabric and was built in collaboration with stellar.org, a non-profit organization and associate member of hyperledger, and KlickEx Group, a regional financial services company in the pacific region. Stellar is an open-source blockchain network that is purpose-built for the issuance and exchange of digital assets. Digital assets are issued on the stellar network as a foreign exchange bridge to allow for near real time settlement. KlickEx group serves as the founding financial institution for the region, servicing banks, retail clients and consumers using this new network.

The network is currently in use by Advanced Pacific Financial Infrastructure for Inclusion (APFII) members, a public-private partnership initially funded by the United Nations and Swift. It is expected to process up to 60 percent of all cross-border payments in the south pacific's retail foreign exchange corridors including Australia, New Zealand, Fiji, Samoa and Tonga by early next year.

IBM Blockchain Platform.

HYPERLEDGER FABRIC

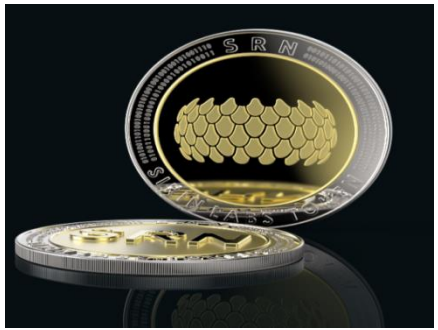
KlickEx Payments without Borders

stellar

Reference: {NSN P569KQ3MSFLS <GO>}

APPLICATIONS TO WATCHES

Huawei technologies ltd., The world's third-biggest handset maker, is considering developing a mobile phone that will be able to run blockchain-based applications, according to two people familiar with the plans.



SIRIN LABS

SIRIN LABS TOKEN(SRN)とは？

特徴、取引所、購入方法を解説

Reference: {NSN P5Y869SYF01S <GO>}

WHERE IS THE BUSINESS VALUE?

- Europe's largest shipping port, Rotterdam, has launched a research lab to explore the technology's applications in logistics.3
- Utilities in North America and Europe are using blockchain to trade energy futures and manage billing at electric vehicle charging stations.
- Blockchain is disrupting social media by giving users an opportunity to own and control their images and content.
- Because we are only now coming to the end of a hot blockchain hype cycle, many people assume that enterprise blockchain adoption is further along than it actually is.

Harvard Business Review

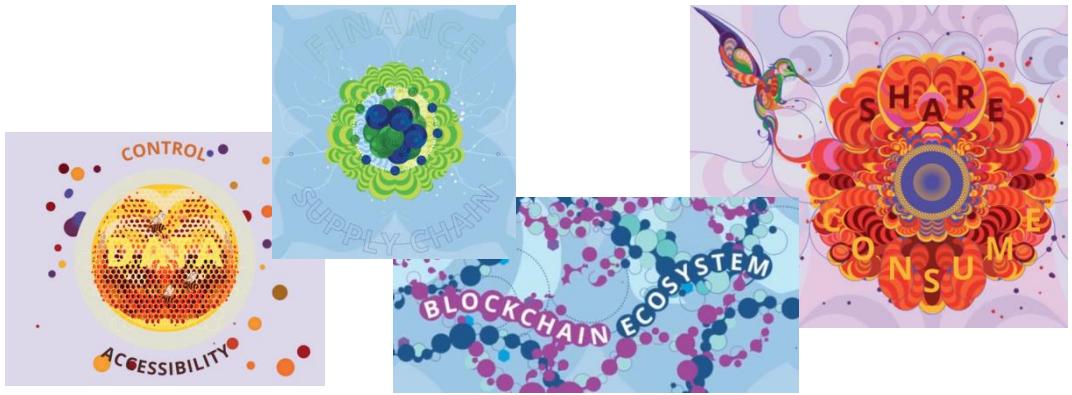
TECHNOLOGY

How Utilities Are Using Blockchain to Modernize the Grid

by James Basden and Michael Cottrell

MARCH 23, 2017 **UPDATED** MARCH 27, 2017

- Another area where blockchain could take hold is in enabling customers to switch power suppliers more quickly. Companies are conducting pilots to explore blockchain's potential to make existing processes, such as meter registration, more efficient and less costly. British startup Electron is developing a blockchain platform that could allow British customers to switch power suppliers reliably within a day, and are working with the Data Communications Company, the UK's new centralized meter data agency. Previously, a switchover could take much longer.



Reference: https://www2.deloitte.com/insights/us/en/focus/tech-trends/2018/blockchain-integration-smart-contracts.html
https://hbr.org/2017/03/how-utilities-are-using-blockchain-to-modernize-the-grid

Q&A

>>>>>>>>>>>>>>>