BERLIN WELCOMES BLOCKSHOW

EUROPE · BLOCKSHOW EDITION · WAY, 2018

COINTELEGRAPH

BLOCK SHOW

POWERED BY COINTELEGRAPH

If you're reading this, you are in the best place for blockchain business!

BlockShow Europe 2018 is not just a platform for efficient networking, high-level knowledge and making profitable deals – it is also an actual show, and we hope it will be a fun and valuable experience for you! Thank you for being with us. Let's begin!

ADDY CREZEE

CEO at BlockShow

AUTOGRAPH

EXHIBITORS

HAB

askfm

NEUROCHAIN

Insights Network

blockhive

izx

edge

KOMODO

Wattle wallet

ICO BOX

EXWAL

GCOX

Signen

Ambrosus

B2expand

PlayHall

BTC.com

Ubex

BIT.GAME

B2 BROKER

BIXBIT

younk

easy MINE

AHEDGEFUND

U Network

traceto.io

HIVE POWER

SPONSORS

ChronoBank.io

Achain

iExec

changelly

ICONIOLAB

UTRUST

DATAVLT

OKEX

weeve

UUNIO

ELVN

INSTASUPPLY

DAKUCE.COM

PARTNERS

BITCOIN MARKET JOURNAL

cryptovest

ICORATING

forklog

CRYPTOSLATE

AMBCRYPTO

BTC-ECHO

DECENT

LATTICE80

Bitcoin Garden

Bitcoin.com

BTCMANAGER.COM

ALL ABOUT THE BITCOIN INDUSTRY

BRAVE NEWCOIN.

Digital Currency Insights

BitNovosti

Все о мире Bitcoin

bitnovosti.com

COINSTELEGRAM

COIN POST

I AM EXPAT

Investing.com

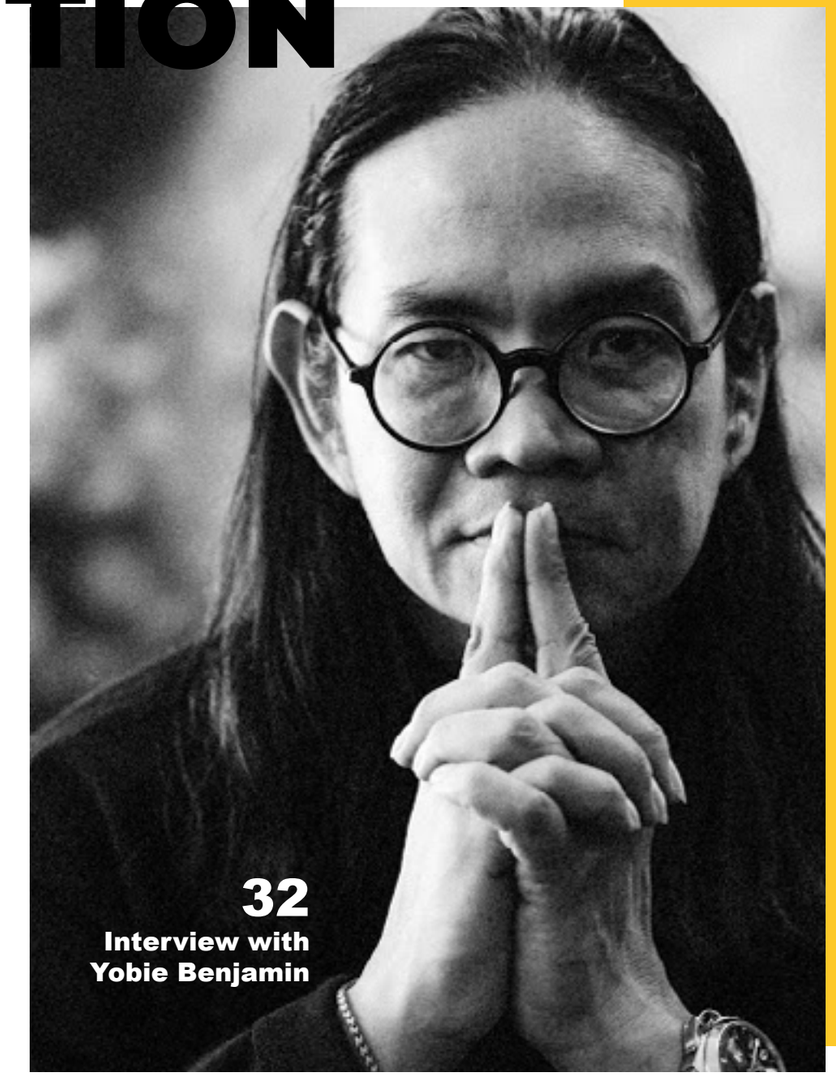
FINTECH SWITZERLAND

GS

CEX.IO

COINTELEGRAPH
The Future of Money

BLOCKSHOW EDITION



BLOCKSHOW

POWERED BY COINTELEGRAPH

MORE FROM LESS

THE STORY BEHIND THE BEST PLACE FOR BLOCKCHAIN BUSINESS

BlockShow here, BlockShow there... people who have ever held this magazine in their hands or surfed the online pages of Cointelegraph have probably heard of numerous events, meetups, and conferences organized by that team. Today, lots of community members know about our recent European meetup tour, as well as the fact that we're expecting some serious tech and crypto celebrities to visit our main conference in Berlin; but who could possibly explain how all of this began?

Well, that's why I'm here. Being in the team since the very conception of BlockShow, I witnessed the formation of the brand – so why not shed some light on this fun and inspiring story?

Everything Begins Somewhere

Let's go back to 2016, a landmark year for the global blockchain community that marked the rapid growth of the ecosystem. This was the year when so many people noticed the technology and figured out all the advantages it could bring to various industries.

Among those inspired by blockchain was Addy Crezee, CEO of BlockShow. By the time the hype was real around blockchain, Addy had already gained some experience working with both blockchain projects and investors interested in those projects. At some point, he realized that the best way of keeping it efficient was organizing events in order to bring the interested parties together. However, this wasn't the only reason:

> *"In May 2016 I got a chance to attend a conference in Helsinki. I made myself a T-shirt saying 'If you want to know about Blockchain, ask me'. Back then, so many people came to me to learn more, to know something new! That was a moment I realized I need to make my own event. The blockchain topic wasn't so mainstream yet, but I wanted to show the community how cool the technology is, how many various sectors it can transform."*

This idea seemed so logical that right off the bat Addy started spreading the word: his own conference would be held in just a few months. According to his words, this news was met with interest and enthusiasm from the community.

The Helsinki Blockchain Conference was held on August 26, 2016, in partnership with Cointelegraph and with the support of many leading companies including Microsoft. Compared to current BlockShow events, the kickoff conference wasn't that impressive when it came to size and scale – but does that even matter? The goal of this debut was to pave the way for further achievements, get a clear understanding of what the audience needs, and set the direction for future activities. Apart from that, the Helsinki Blockchain Conference enabled us to make wonderful friends and partners who support BlockShow to this day.

The Helsinki Blockchain Conference, which brought together more than 200 attendees, was a moment of truth that led us to BlockShow as we know it. The name itself came about for a special reason – even at the very beginning, our credo was not to be just another corporative gathering, but to become a place that would combine a whole spectrum of opportunities for efficient business development and networking with a relaxed atmosphere and community-friendly environment.

How are things going today?

There's not much sense in retelling the recent history of BlockShow. Right after the brand's first big conference, BlockShow Europe 2017, the team (as well as the event itself) began to grow; BlockShow caught its own wave, and since then, its main aim has been to keep increasing the scale, to perfect every single element, and to become truly global – this is exactly what BlockShow has been doing for the past year.

> *"Now, a year later, I'm really shook – it was like the whole five years to me! I realize that we've grown up so much: from the small 500-people event, we walked our way to the large team of more than 30 workers globally. We are making tens of events every year – both small and big ones – and there's no doubt for me that we'll become the world's major Blockchain event in 2018. A year later, I understand how much we've done, and this year we'll do more than ever. We will lay the foundation of the whole industry."*

Looking Ahead

What can I say in conclusion? It's clear that the story of BlockShow is open-ended; so many objectives to achieve, so many heights to scale... and I personally have the most positive expectations. I'm sure that BlockShow's triumph is still to come, and I hope that, some time in the future, you and I will meet at another BlockShow conference, take a look around, and assess the truth of my wishful thinking. :)

BLOCK SHOW

POWERED BY COINTE

BUBBLEMANIA

IS CRYPTO SPACE FATED TO BECOME ANOTHER DOTCOM BUBBLE?

The cryptocurrency craze in 2017 saw the prices of crypto tokens rise to tens of thousands of times their original values. Bitcoin wasn't the only token to reach its all-time high – even the prices of altcoins like Ethereum, Cardano, Ripple, Stellar, and NEO were all buoyed to new heights by the increased demand from investors seeking to take a piece of the action. The cryptocurrency market hit a peak of total capitalization of nearly $800 bln in January 2018.

The market's meteoric rise had many, especially those from traditional investing, calling the phenomenon a "bubble." Since people try to make sense of new events using the past, the crypto space has been commonly viewed through the lens of the "dotcom crash" in the late 1990s to the early 2000s. Hundreds of companies met their ends in the aftermath of the so-called "dotcom bubble."

SO, IS THE CRYPTO SPACE HEADED DOWN A SIMILAR PATH?

Still a Frontier

The crypto space can still be considered a frontier. Blockchain as a technology is only gradually starting to see wider adoption. There are still a few regulations in place to keep ventures and participants in check. The market trades heavily on speculation. Most projects behind crypto tokens have even yet to actually show or deliver definitive real-world value.

It seems to be difficult to pin down the basis of what's driving the performance of cryptocurrencies. Support can shift easily from one project to another even if there isn't much fundamental basis for a token's sudden climb.

It's also tough to anticipate how certain events would impact the market. For example, many would have expected for Chinese blockchain projects to have a hard time considering the country's ban on initial coin offerings (ICOs). This ban, however, appears to have been quite advantageous for ventures like NEO. Since the platform's launch preceded the ban, it essentially avoided being used by scam projects that have emerged. Support for the project is growing, and NEO's social hype and price movement even showed resilience when Bitcoin dipped.

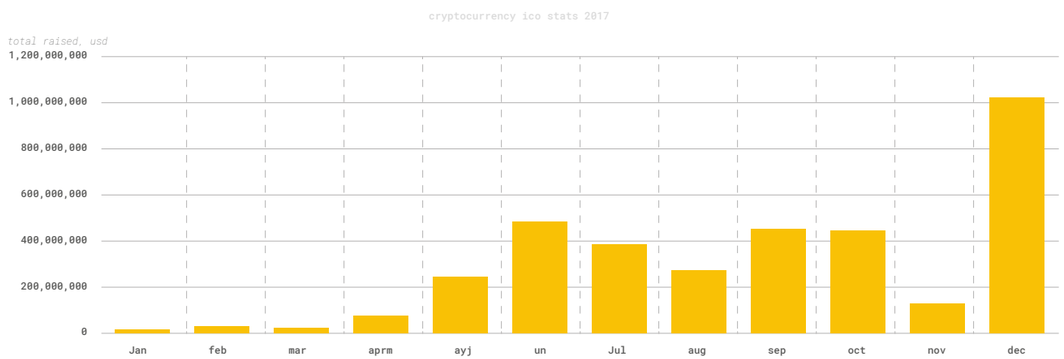
Understandable Comparison

Economic bubbles are formed when assets are being traded at prices that are significantly more than their intrinsic values. The crypto market's highly speculative nature has definitely contributed to the overvaluation of a number of cryptocurrencies. For instance, Dogecoin, a joke currency, has a market capitalization of over $323 mln at the time of writing. It even reached over a bln dollars at its peak – an astounding achievement for a project meant to be nothing more than a parody.

So, by traditional definitions, there are bases to call what's happening to cryptocurrencies a bubble. As such, it's only natural and considerably fair to compare it to the dotcom bubble since it's the most recent one that involved disruptive technologies. Both have displayed similarities in their respective build-up of events.

Arrival of disruptive technologies. The emergence of accessible personal computing, commercial Internet Service Providers (ISPs), and better web browser technology created a consumer market for internet companies. Internet adoption in the 90s also experienced rapid growth. As for crypto, blockchain has been around for longer prior to this cryptocurrency boom. The use of distributed ledger technology had been proposed from more than a decade back. It was only until recently with the buzz surrounding Bitcoin and the introduction of platforms like Ethereum that it found more applications. Traditional institutions legitimized the technology by embarking on blockchain projects themselves.

Explosion of ventures. Both events featured the sudden explosion of projects and ventures looking to capitalize on the technology. Hundreds of companies were founded during the dotcom craze. In 1999, there 457 initial public offerings (IPOs) most of which were tech companies. In March 2000 during the market's peak, there were 4,715 companies trading on Nasdaq. The crypto industry is experiencing something similar with ICOs. In 2017, CoinSchedule logged 210 ICOs, up from just 43 in 2016. These ICOs raised more than $6 bln in funding. So far in 2018, there have already been more than 70 token sales.



Sharp climb in stock/token prices. The share prices of Internet companies skyrocketed while the dotcom industry was developing. Of the IPOs in 1999, 117 companies doubled their share prices just on the first day of trading underscoring the exuberance of the market. Nasdaq peaked in March 2000 hitting an intraday high of 5,132. Crypto tokens display even more gains. It isn't uncommon in the crypto market to see tokens rise to hundreds of times their prices at ICOs in just a matter of months.

These are the patterns that lead many to believe that crypto's trajectory is the same. The dotcom bubble burst sometime in 2002, and the Nasdaq bottomed out in September 2002.

Recent events seem to imply a similar outcome. In February 2018 a massive correction occurred that saw Bitcoin's price tumble down to the $6,000 mark. Other coins also took major hits. The total market capitalization dropped by more than 60 percent from the peak to around $265 bln. Many thought that this was the bubble bursting. Analysts even warned that Bitcoin would go below the $1,000 mark. Token prices have been pretty volatile throughout March and haven't found a bottom for the time being.

Lessons to Be Learned

Noam Levenson, CEO and co-founder of Eden Block, shares:

> ***"So, the real question is not: are we in a bubble? But rather, how big will the bubble get? If we respect the natural evolution of disruptive technology, then we must understand that with every massive speculative run-up, there is an equally massive crash. From the tulip bubble of the 1600s to the Internet bubble only 15 years ago, the crashes are inevitable. Thus, the question is, what can we learn from past bubbles, and how much can they guide our actions within the cryptocurrency market?"***

The case of Pets.com, the poster child of what went wrong during the dotcom bubble, should contain plenty of lessons for crypto stakeholders. The arrival of the Internet encouraged companies to pursue direct-to-consumer e-commerce efforts. Pets.com sought to sell pet accessories and supplies much like how Amazon sold books through online channels. The company was also able to attract venture funding that inflated its valuations.

However, the company had a poor business model and had no independent market study to ensure its sustainability let alone its profitability. The company failed to make ends meet. Trying to absorb the high shipping costs of heavy pet supplies like pet food and cat litter was clearly more than an oversight.

The crypto space is already seeing similar poorly-planned me-too ventures emerge. It seems like companies are trying to tokenize everything using blockchain withouting considering if the technology is mature enough to handle a particular use case or if these ventures' targeted objectives have any real need for the decentralized technology.

However, blockchain ventures can't be taken in exact comparison. Here are some key differences in how they operate:

Zero to minimal logistics. A lot of dotcom companies were forced to balance running both online channels and physical fulfilment. Many found themselves overwhelmed by logistics like the case of Pets.com, eToys, and Webvan. Blockchain projects deal with mainly digital transactions and tokenized assets. Unless the venture seeks to omnichannel or brick-and-mortar presence, most services interaction layer, there are minimal logistics concerns.

Smaller workforce. Since many dotcom companies had to deal with physical fulfilment, they had to hire a large number of employees to deal with warehousing and logistics on top of their development, sales, and marketing staff. Most blockchain teams are lean and mean. Most can even easily operate remotely lessening the need to put up physical offices and infrastructure.

Comfort with technology. Market-wise, crypto ventures also have demographics on their side. Dotcom companies had to deal with technological migrants in the boomers and Gen Xers forcing them to allot resources for client education and after-sales support. Millennials are now the dominant demographics. Participants in the crypto market are now comfortable using digital channels for big-ticket transactions.

Innovation and Sustainability

While it is only prudent and smart for anyone entering the crypto space to proceed with caution especially when it comes to trading and investing in crypto assets, it would be unfair to be totally dismissive of what blockchain technology has brought about. The parallels with the dotcom bubble should serve as lessons to stakeholders.

One must remember that the aftermath of the dotcom bubble also affirmed that truly innovative organizations and technologies could weather the storm. Companies such as Amazon and eBay proved that pairing novel ideas with good business acumen can lead to success.

Surely, the situation today with crypto and the environment of dotcoms from nearly twenty years ago would have their differences. Ventures must be able to navigate these nuances in order to make the best possible decisions moving forward. Whether or not crypto ventures will share a similar fate to dotcoms remains to be seen. At least for now, crypto stakeholders have a chance to write a different story

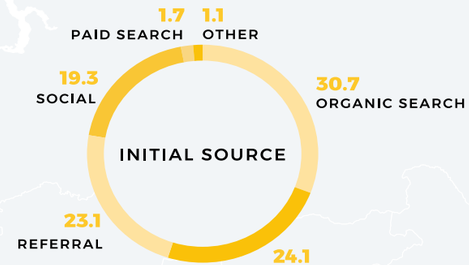
STATS

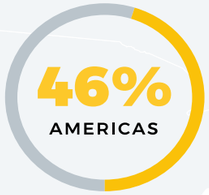
COINTELEGRAPH

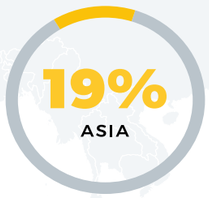
MEDIA GROUP STATS

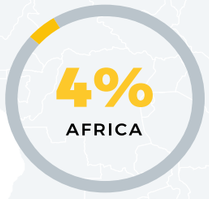
879 000 000
PAGE VIEWS PER MONTH

117 000 000
UNIQUE VISITORS









25 000
SUBSCRIBED
TO DAILY NEWSLETTER

9 000 000
UNIQUE VISITORS

77 000 000
PAGEVIEWS PER MONTH

COINTELEGRAPH
The Future of Money

TECHNOLOGY

ETHEREUM COMMUNITY CONSIDERS HARD FORK TO FIGHT ASIC MINERS

Ethereum developer Piper Merriam opened the Ethereum Improvement Proposal (EIP) #958 on Github on March 30, presenting the idea of a possible hard fork in the Ethereum (ETH) protocol to invalidate ETH ASICs.

Vlad Zamfir, another developer at the Ethereum Foundation, posed the same question on Twitter on March 28. 57 percent of respondents voted yes to the idea of a hard fork.

Both developers' polls emerge amid rumors that the Chinese ASIC manufacturer Bitmain is on the brink of shipping its first Ethash compatible ASIC miners. Ethash is the Proof-of-Work (PoW) hashing algorithm used by Ethereum and a variety of other altcoins.

Buterin's Ethereum white paper suggests the protocol already has a twofold resistance to mining centralization.

Firstly, the algorithm requires miners to return the hash for data that has been "randomly selected" from transactions in the preceding block. Since "Ethereum contracts can include any kind of computation," "an Ethereum ASIC would essentially be an ASIC for general computation – i.e. a better CPU."

The second means of defense is to "poison the well," which Vitalik characterizes as "ultimately an adaptive human solution rather than a technical one." If a certain type of computation becomes prevalent, then conventional miners can introduce "a large number of contracts into the blockchain specifically designed to stymie certain ASICs".

As Cointelegraph reported in February 2018, Bitmain's profits outstripped the US GPU giant Nvidia in 2017. Research by Bernstein analysts estimated Bitmain's profits to be between $3-4 bln for 2017, holding 70-80 percent of the market for Bitcoin miners and ASICs.

Ethereum's informal poll regarding a possible hard fork follows Monero's rejection of centralized hashpower last month. Monero's lead developer Riccardo Spagni warned that the coin's protocol would be changed every six months to stymie ASIC monopolies. Rumors regarding possible deployment of Ethash compatible ASIC miners impacted Ethereum markets, according to some commentators.

> ***Ethereum contracts can include any kind of computation.***

GILLES FEDAK
CEO & CO-FOUNDER OF IEXEC

EXCLUSIVE INTERVIEW FOR BLOCKSHOW EUROPE 2018

JEAN-CHARLES CABELGUEN
CHIEF INNOVATION & ADOPTION AT IEXEC

GILLES FEDAK
CEO & CO-FOUNDER OF IEXEC

iExec is the first decentralized marketplace for cloud resources. Tell us more about your project.

Back in April 2017, iExec was the fifth biggest ever at that time. We celebrated the first anniversary of the RLC token sale a few weeks ago. Since then, we released the first version of the iExec SDK in November 2017, along with a Dapp Store and a dedicated explorer. It's running on mainnet since December and the team is now made up of 20 people who worked pretty hard to deliver the version 2 of our product today.

We're releasing the first marketplace for cloud computing resources – servers and applications can trade their computation power like they would trade any other commodity. Workers (servers) directly earn some value by selling their computation power on the market. On the demand side, applications and users have easy and affordable access to those resources.

At iExec, we believe that decentralization is the future of the Internet. Our goal is to provide the infrastructure that will sustain this decentralized economy.

WHAT IS THE LATEST NEWS FROM IEXEC?

The RLC token is now listed on all major exchanges and the community is growing fast. The first metrics we have on adoption are very encouraging. We announced the result of the Dapp Challenge a few weeks ago: we selected 15 applications and they're delivering. We now have about 50 apps registered on the Dapp Store.

We sealed several key partnerships with resource providers like Stimergy, Genesis Mining, Cloud & Heat and Nerdalize, and we're happy to announce that Alibaba Cloud will be part of the providers of the network.

In addition to that, we recently announced a partnership with Ubisoft, one of the major players in the gaming industry. On the R&D side of the project, we are collaborating with Intel on SGX technology that we plan to use to provide a satisfying level of privacy.

WHAT PLANS DOES IEXEC HAVE FOR 2018? WHAT'S GOING ON RIGHT NOW IN IEXEC'S DEVELOPMENT?

Every two weeks, we publish a 'Development Letter' to give as many details as we can on what's been done. In my opinion, it's extremely important to keep our community updated on what we are doing. The marketplace is running on Ethereum mainnet. It includes the 'Proof-of-Contribution' or 'PoCo': PoCo is the consensus protocol iExec uses to verify the result of an off-chain computation.

In 2018, we will gradually open the platform to public worker pools so that anyone can contribute to the network; you will also see data providers joining the network. Since iExec is 'blockchain agnostic', our product will be compatible with other blockchains.

WHAT EXPECTATIONS DO YOU HAVE FOR BLOCKSHOW EUROPE 2018? WHAT'S YOUR MAIN GOAL FOR SUPPORTING AND PARTICIPATING IN THE EVENT?

Our objective is to stimulate offers and demand in the marketplace, so we're looking for different kinds of partners: server providers as well as applications in need for affordable computing power. We also want to open discussions with exchanges, crypto funds and other important players in the industry.

When a smart contract needs to launch some off-chain computation, you can think of iExec. If you want to add a powerful feature to your decentralized application, you can do it for free with iExec.

BlockShow Europe 2018 is a great opportunity for us to showcase our product, present it to attendees, and also participate in discussion panels to share our experience of distributed networks with the whole crypto community.

READ ME

ESSENTIAL KNOWLEDGE ABOUT SMART CONTRACTS

SMART CONTRACTS: WHAT ARE THEY AND WHY SHOULD WE CARE?

Nobody likes a middleman – they often take our time and money to do things that we could probably do ourselves, and we never know if they really have our best interests at heart. In the 21st century, the age of technological enlightenment, do we really even need them anymore?

Smart contracts not only remove the cost and conflict of interest issues possible by using an intermediary but ensure that the transaction of our assets over the blockchain is secure and transparent by defining and automatically enforcing the terms of a deal. The agreements are converted into code and just like any other decentralized system, they are monitored by the network of computers that operate the blockchain. It is a dependable system, but as with most things, real trust comes from a place of understanding.

Here, we will help you to understand the code behind smart contracts.

Let us analyze the example of Zero Ex to better understand the essence of smart contracts.

Zero Ex Intl provides a platform for the decentralized exchange of ERC20 tokens. It is worth noting that most crypto-asset exchange platforms are still centralized. The Zero Ex protocol allows participants to transfer ERC20 tokens between themselves in a secure and transparent way through an Ethereum smart contract. The project has already raised $24 mln through initial coin offerings (ICOs).

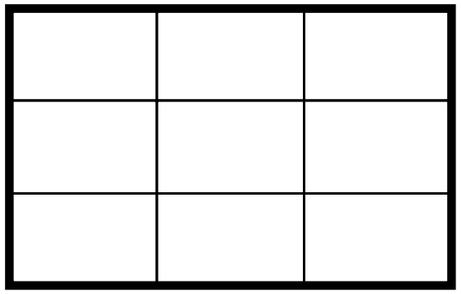
There are some symbols, which are important to know. “///” at the beginning of a line signifies a developer’s comment, which ends at the end of the line. All smart contracts consist of special functions. A smart contract begins with a brief function description, and said functions are usually explained by the smart contract writer. They can outline a function’s parameters and detail its elements. “@” precedes the name of an element. For example, “@flowers – the number of flowers that could be used”. The “@” symbol also signifies a developer’s comment. Further examples are below.

THE STRUCTURE OF GENERAL TOKEN SMART CONTRACTS

A simple smart contract is usually comprised of several contracts arranged in a hierarchy. At the top of this pyramid is the contract token, in which all of the smart contract's functions are detailed. Every subordinate smart contract provides more information about the functions and can even introduce new functions. All functions should be covered in the smaller contracts.

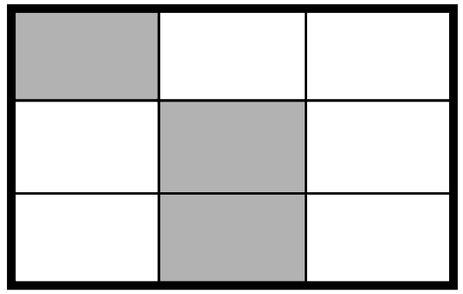
The structure of an ordinary smart contract can be represented as a table. The whole table would be a contract token, and the table cells are functions. Subsequent contracts are represented by filling cells.

1



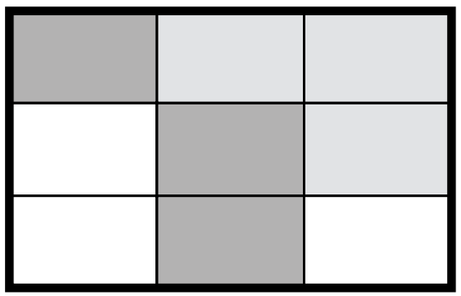
CONTRACT TOKEN (EVERY CELL IS A FUNCTION)

2



CONTRACT STANDARD TOKEN BUILT ON A CONTRACT TOKEN COVERS A FEW FUNCTIONS AS SHOWN IN THE TABLE ABOVE

3



SMALLER CONTRACTS BUILT ON A CONTRACT STANDARD TOKEN COVER ADDITIONAL FUNCTIONS AS SHOWN IN THE TABLE ABOVE

4

THE LAST CONTRACT IN THE HIERARCHY COVERS LAST UNCOVERED FUNCTIONS.

Most token smart contracts are built the same way. As you can see above, the ordinary contract token alone is not a real working program, as it does not work without smaller contracts built on it. In addition, smaller smart contracts could not exist without the contract token.

If any function is not represented in one of the contracts, the whole smart contract will not work. Therefore it is very important that every function mentioned in the contract token is covered by the smaller contracts.

By reading the first part of any smart contract, you gain a general understanding of the smart contract in its entirety.

ADDITIONAL COMMENT	SMART CONTRACT	EXPLANATION
contract token is a "table" as mentioned below	contract Token {	
N.B. "param" means indication of some parameter. @param_fl could be	// @return total amount of tokens	
First cell	function totalSupply() constant returns (uint supply) {}	General function of supplying tokens. It is quite widespread.
N.B. "param" indicates a parameter, some number which would be indicated in real case. Every "param_" has the same meaning below.	/// @param _owner The address from which the balance will be retrieved	Explanation of term which could be used in more detailed and technical description of function.
Second cell	/// @return The balance	Explanation of what the word "return" refers to.
	function balanceOf(address _owner) constant returns (uint balance) {}	This phrase should be understood like so: we specify an "address_owner" and the function outputs the "unit balance"
	/// @notice send `_value` token to `_to` from `msg.sender`	Explanation of the relationships between "_value", "_to" and "msg. sender"
	/// @param _to The address of the recipient	Explanation of "param _to"
	/// @param _value The amount of token to be transferred	Explanation of "param _value

	/// @return Whether the transfer was successful or not	What will be returned to the participant after doing the function
Third cell. Bool success is a logical function which has two possible outputs: “true” or “false”, here and below.	function transfer(address _to, uint _value) returns (bool success) {}	The function sends some units and informs us whether it is successful or not
	/// @notice send `_value` token to `_to` from `_from` on the condition it is approved by `_from`	We can see that the comment is very similar to the first comment of function transfer. The difference is a new condition “approved by sth”. Functions "transfer" and "transfer from" look very similar. However we can see the difference in new detail "approved by '_from' "
	/// @param _from The address of the sender	Explanation of “param _from”
	/// @param _to The address of the recipient	Explanation of “param _to”
	/// @param _value The amount of token to be transferred	Explanation of “param _value”
	/// @return Whether the transfer was successful or not	What will be returned to the participant after performing the function
Fourth cell	function transferFrom(address _from, address _to, uint _value) returns (bool success) {}	As mentioned below, the function “transfer from” is very similar to the function “transfer”.
	/// @notice `msg.sender` approves `_addr` to spend `_value` tokens	Passing of the right of transfer from one participant to another
	/// @param _spender The address of the account able to transfer the tokens	Requirement for being “param _sender”

	/// @param _value The amount of wei to be approved for transfer	It is quite obvious: how many tokens could be transferred
	/// @return Whether the approval was successful or not	What will be returned to the participant after performing the function
Fourth cell	function approve(address _spender, uint _value) returns (bool success) {}	Function “approve” makes a participant able to transfer tokens (unit value) from another participant’s count
	/// @param _owner The address of the account owning tokens	Explanation of “param_owner”
	/// @param _spender The address of the account able to transfer the tokens	Explanation of “param_spender”
	/// @return Amount of remaining tokens allowed to spent	How many tokens the spender allows to transfer from their account.
Sixth cell. We will check that all functions have been implemented	function allowance(address _owner, address _spender) constant returns (uint remaining) {}	There is slight difference between “function allowance” and “function approve”. “Function approve” implies that the active participant is someone who consents to the transfer of their tokens. “Function allowance” implies that the active participant is someone who receives the permission. Actually, the function is an opportunity to find out how many tokens are approved for the asking participant.
We should see the event like a part of an observable pattern. A smart-contract can show an "event". All those who follow the update of the smart-contract’s general Blockchain will see this event.	event Transfer(address indexed _from, address indexed _to, uint _value);	There are no comments for the event “Transfer” from the SmartContract author. So we need to guess what does the event does. The event is based on “address indexed_from” “address indexed_to”, uint_value. Obviously, the event will inform how many tokens were transferred from “address indexed_from” to “address indexed_to”

```
event Approval(address indexed _owner, address indexed _spender, uint _value);
```

There are no comments for the event “Approval” from the SmartContract author either.

```
}
```

```
contract StandardToken is Token {
```

A beginning of detailed procedure description

Presented third “cell”. There are 1st, 2nd, 4th, 5th, 6th cells which should be represented.

```
function transfer(address _to, uint _value) returns (bool) {
//Default assumes totalSupply can't be over max (2^256 – 1)
if (balances[msg.sender] >= _value && balances[_to] + _value >= balances[_to]) {
balances[msg.sender] -= _value;
balances[_to] += _value;
Transfer(msg.sender, _to, _value);
return true;
} else { return false; }
}
```

The essence of the function Transfer is revealed. Firstly, the author mentions the maximum total supply. The function is a simple conditional statement. If all conditions (balance of message sender is high enough for spending, the value is not negative) are met, the function will give the output “true”. If they are not met, function will give the output “false”.

```
/* A contract attempts to get the coins */
function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
    if (balanceOf[_from] < _value) throw;                 // Check if the sender has enough
    if (balanceOf[_to] + _value < balanceOf[_to]) throw;  // Check for overflows
    if (_value > allowance[_from][msg.sender]) throw;   // Check allowance
    balanceOf[_from] -= _value;                           // Subtract from the sender
    balanceOf[_to] += _value;                             // Add the same to the recipient
    allowance[_from][msg.sender] -= _value;
    Transfer(_from, _to, _value);
```

Presented fourth “cell”. There are 1st, 2nd, 5th, 6th cells which should be represented.

```
function transferFrom(address _from, address _to, uint _value) returns (bool) {
if (balances[_from] >= _value && allowed[_from][msg.sender] >= _value && balances[_to] + _value >= balances[_to]) {
balances[_to] += _value;
balances[_from] -= _value;
allowed[_from][msg.sender] -= _value;
Transfer(_from, _to, _value);
return true;
} else { return false; }
}
```

The function “transferFrom” is a simple conditional statement too. The content of the function is similar to the function “transfer” as we have already noted above. The function “transferFrom“ compares the transferred value with the allowed value.

Presented sixth “cell”. There is 1nd cell, which should be represented.

```
function allowance(address _owner, address _spender) constant returns (uint) {
return allowed[_owner][_spender];
}
```

the opportunity for “address _spender” to find out how many tokens are approved for him

```
mapping (address => uint) balances;
mapping (address => mapping (address => uint)) allowed;
uint public totalSupply;
}
```

linking two data sets: addresses and amounts of tokens

```
contract UnlimitedAllowanceToken is StandardToken {

uint constant MAX_UINT = 2**256 – 1;

/// @dev ERC20 transferFrom, modified such that an allowance of MAX_UINT represents an unlimited allowance.

/// @param _from Address to transfer from.

/// @param _to Address to transfer to.

/// @param _value Amount to transfer.

/// @return Success of transfer.
```

Comments to the “param_s” are already mentioned above. The function “transferFrom” is a conditional statement with several initial data, like “unit_allowance”, “value” and “balance_to”. It is completed if the “Balance from” value is not negative.
This function considers allowing the transfer of more tokens than were initially issued. It looks strange, but the developer does it to give you the opportunity to share your account forever. If you allow the transfer of a larger sum of tokens than was issued to participant 1, the amount of tokens permitted for participant 1 will never decrease.

N.B. “cell” 4 occurs for a second time. It means that the function “transferFrom” operates under the new rules from now.

```
function transferFrom(address _from, address _to, uint _value)

public

returns (bool)

{

uint allowance = allowed[_from][msg.sender];

if (balances[_from] >= _value

&& allowance >= _value

&& balances[_to] + _value >= balances[_to]
```

N.B. “cell” 4 occurs for a second time. It means that the function “transferFrom” operates under the new rules from now.

```
) {

balances[_from] -= _value;

if (allowance < MAX_UINT) {

allowed[_from][msg.sender] -= _value;

}

Transfer(_from, _to, _value);

return true;

} else {

return false;

}}}
```

It easy to confuse “function transfer” with “Transfer”. “Function transfer” is a “cell”, “Transfer” is an event, the type of code part is mentioned in the first part of the smart-contract

The last contract in the hierarchy. It is very important to read it scrupulously. It should not consist of fraudulent function changes, like changing the function body to transfer all tokens to a third-party address.

```
contract ZRXToken is UnlimitedAllowanceToken {

uint8 constant public decimals = 18;

uint public totalSupply = 10**27; // 1 billion tokens, 18 decimal places

string constant public name = "0x Protocol Token";

string constant public symbol = "ZRX";

}}}
```

The last contract tells you how many symbols are available. It generally includes the token name and an indication of the total token amount.

Any questions that arise while reading through the details should be put to a smart contract writer through any direct channel, for example on BitCoinTalk. If the author ignores the question or provides a vague, general answer, this should be a red flag to the prospective investor.

LEGAL

FRANCE AND GERMANY

HOW REGULATORY PRACTICES IN THE TWO COUNTRIES COULD AFFECT EU LEGISLATION

The first meeting of G20 finance ministers and central bank governors this year was highly anticipated by the crypto community after a series of inconsistent words and regulatory frameworks among the world's biggest players. However no joint framework declarations came out of the meeting.

The first meeting of G20 finance ministers and central bank governors this year was highly anticipated by the crypto community after a series of inconsistent words and regulatory frameworks among the world's biggest players. However no joint framework declarations came out of the meeting.

With the Financial Stability Board's cautious statements casting chill over individual members' enthusiasm to discuss crypto matters, all that came out of the summit was merely a bunch of baby steps in the anticipated direction. Once again, the community is left to do what it has been doing all along: interpreting subtle cues and contradictory signals that emanate from policymakers in individual nation-states.

France, one of the vocal proponents of cryptocurrency regulation at the G20 level, has been a major hotbed for contradictory signals. In a recent about-face, The Autorite des Marches Financiers (AMF) unveiled a set of new initial coin offering (ICO) rules that appear extremely lenient towards both entrepreneurs and investors. The development came across as utterly unexpected, especially given the fact that merely days before the announcement the AMF cracked down on 15 crypto-related websites for unlawfully marketing investment services.

Germany is another European powerhouse which has proposed a unified approach to crypto regulation earlier this year. Much like its neighbor, Germany seems to be swinging its view – though in a less dramatic way. Having issued a series of warnings regarding the speculative character of cryptocurrency trading and ICO investments in November 2017, German authorities are now clarifying some of their stances and issuing promising signs.

As the European Union's (EU) dominant powers, this duo will likely lead the way in crafting any potential EU-wide standards for governing blockchain and the wealth of

its applications. Despite stark distinctions in the way their legal systems and regulatory regimes operate, in recent decades France and Germany have exhibited quite a few common patterns in handling new regulatory challenges brought about by the rise of internet industries.

From limiting online speech to protecting user data to levying taxes on tech giants, both countries have demonstrated a tremendous appetite for asserting their sovereignty over the online realm. Presuming that the spirit of broader Internet governance is highly likely to carry over to blockchain regulation, a closer look at the already established patterns is useful for envisioning what the imminent cryptocurrency related policies might look like.

INFRASTRUCTURE & ISPS

One thing to remember about continental Europe is that historically, the role of the state and centralized bureaucracy has been greater than those in common law-based Anglo-Saxon systems. The tradition of statutory law along with corporatist political culture prescribed not just an overall embrace, but expectation of active regulatory involvement on behalf of the state in the most important spheres of domestic policy. Both states have certainly lived up to these expectations.

The French government has been directly managing communication networks since the very early stages of their mass expansion. The first network to connect vast numbers of French people was not the Internet but rather the homegrown and highly centralized Minitel. Once the functional superiority of the global network became evident to the government, it took measures to boost Internet adoption – again, via a state program. Content blocking requirements are embedded into legislation, and it is Internet Service Providers (ISPs) that are held liable for violations. ISPs do engage in some degree of self-regulation, but usually government intervention precedes any self-imposed restrictions. Blocking is amply used to enforce copyright and prevent illicit activities such as unlicensed gambling or the distribution of content depicting child abuse.

A vastly different set of domestic rules and practices is in place in the German system, where the idea of "regulated self-regulation" took hold. At least in part, it emerged as an unintended consequence of German federalism: while the debate as to whether policing web content should be a prerogative of national or federal authorities dragged for years, ISPs were able to use this time to put together a working system of industry associations. A part of this system is a self-regulatory authority that partners directly with search engines. As a result, no direct blocking by the government exists since filtering of content happens at the stage of indexing. ISPs are not held liable for illegal content that travels through their pipes. Communication industries command a powerful network of organized interests that is strongly opposed to censorship.

ONLINE SPEECH REGULATION

France and Germany have both embraced a similarly aggressive stance in policing some forms of online expression. French law criminalizes racist and anti-semitic speech both offline and online; each new government routinely puts forward a new comprehensive state program to fight hate speech in the public sphere. State officials' faith in power of direct content regulation seems to be unfailing: for one, President Emmanuel Macron pledged in January 2018 to roll out an anti-fake news law by the end of the year.

The German legislative quest against hate speech culminated in the 2017 "Facebook law," which imposed heavy penalties on social media platforms for failing to quickly remove illegal content from public view. Facebook and Twitter responded by fielding record numbers of German-speaking moderators in early 2018. The effects of these mutual accommodations are yet to be seen. Meanwhile, German law enforcement occasionally surprises particularly bad-mouthed folks with raids on their homes.

PERSONAL DATA

Another similarity between the two countries has been the degree of protection afforded to internet users' personal data, as well as their willingness to enforce this protection vis-à-vis Facebook and Google. Germany's competition-regulating authority has gone after Zuckerberg & Co, citing alleged abuse of their dominant position in the personal data market. France took issue with Facebook's apparently shady practices of harvesting WhatsApp users' data without consent.

A different privacy battle, now against Google, unfolded over the EU law granting users the "right to be forgotten" – a requirement for search engines to remove URLs containing irrelevant or outdated personal information upon individuals' requests. A court in Munich issued an order demanding that Google's URL takedown procedure be changed in a way that does not allow the purged links to resurface as easily as they do now. Meanwhile, France's lawsuit against the search giant, seeking to extend the right to be forgotten to jurisdictions outside of the EU, will be heard by the EU Court of Justice after three years of litigation in the lower courts.

FISCAL POLICIES

GAFA is an acronym that EU policymakers often use to refer to global – essentially, American – tech giants with a massive European presence. Even though it originally stands for Google, Apple, Facebook, and Amazon, the term has come to refer to any platform of comparable size, used mainly with regard to the need for holding them accountable. Taxation is one GAFA issue that European politicians have been hammering on throughout most of 2017 and early 2018. It is no secret that big tech companies have been ingenious in minimizing their tax obligations on their European profits for years, but now it appears that enough is enough for the EU.

Germany and France have already tackled the issue at home: both nations introduced taxes on video distributors like YouTube and Netflix, with proceeds flowing to support production of local content. The French government now seeks to advance EU-wide rules whereby digital companies would be taxed on revenues rather than profits, a move that will presumably alleviate the practice of registering the profits in low-tax EU jurisdictions instead of where they were earned. A ruling coalition in the German parliament proposes a slightly different solution: a consolidated tax system proportionately allocating companies' European profits according to the geographic location of their customers. Regardless of whichever approach ultimately prevails, there is little doubt that the days of GAFA's European tax havens are numbered.

TAKEAWAYS

However peculiar and novel cryptocurrency regulations may seem, it does not emerge in a vacuum. Like any other sphere of governance, it bears the spirit and coloration

of the wider system of legal control within which it operates. The story of Switzerland is canonic in this sense: it is hardly surprising that a country with traditionally little government presence and a tremendous record of accumulating and managing foreign wealth is emerging as a booming crypto hub.

As Marc P. Bernegger, Swiss crypto entrepreneur and Board Member of the Crypto Finance Group in Zug, put it in an interview for Cointelegraph:

> ***"Switzerland has in general a very liberal approach and far less rules and regulation than other countries. With our direct democratic system, the whole government is already decentralized, which seems to be one of the reasons for its crypto friendly behavior. (...) Today, literally every week there are several new blockchain companies moving to 'Crypto Nation' Switzerland."***

However, a principle that seems so intuitive in the Swiss case is less frequently invoked with regard to France and Germany. As common wisdom places them both in the line of "progressive" liberal nations, many in the crypto community anticipate some latitude to be afforded by these governments. However, the ways in which French and German authorities have been handling tech industries suggests that we should be modest in our expectations.

Both states clearly have a penchant for regulation. Regardless of whether it is a direct legislative control in the French style or a more "distributed" regulatory system akin to the German one that is employed for domestic use, on the outer flank European nation-states are equally protective of their sovereign realms. In the face of global forces tapping into their jurisdictions, both Germany and France prefer to act aggressively, whether it has to do with protecting citizens' personal data or levying taxes on digital platforms. Additionally, security concerns over financing hate groups or terrorist activities could potentially yield restrictive outcomes. All in all, even when the signals that come from the European powerhouses are positive, blockchain entrepreneurs should not be quick to celebrate: there might still be strings attached.

On the bright side, involvement of the State in defining the rules of the game is not necessarily a dreadful thing. Since this is not a zero-sum situation, a meaningful dialogue between policymakers and organized industry interests may give rise to arrangements that make sense to all. At least in Germany, such a dialogue seems to be taking place. According to Blockchain Bundesverband, an advocacy group that advances the interests of the German crypto community, the government has begun to address blockchain regulation in earnest. Dr. Nina Siedler, who is leading the organization's Token/Finance working group, sounded optimistic on the matter:

> ***"The community wants fair rules, a level field for everyone. Most of the issues are covered by the existing laws, but the problem is that some of the rules are not very specific. The government's presence in this process is not obtrusive, they don't want to overregulate. They clearly want to give this rising economy a chance."***

Dr. Siedler also suggested that some of the "grey zones" in blockchain governance might well be addressed by a coordinated self-regulatory effort. She mentioned that a Europe-wide initiative is currently underway to formulate a blockchain entrepreneur's code of conduct, a set of best practices that will delineate the foundational tenets of the industry's self-governance. This development offers some hope with regard to the future of European crypto regulation. As the case of the German ISPs illustrates, putting up organized interests early in the process of exploring uncharted policy area has a potential to put the whole industry in an advantageous position down the line.

‘I’M QUITE A FAN OF GOVERN-MENT REGULATION’

YOBIE BENJAMIN

> ***Regulation actually legitimizes a business.***

In the corridors of Davos Cointelegraph got a chance to catch up with Yobie Benjamin, co-founder and CTO Emeritus of Token.io, who also has a background in mainstream banking (Citigroup).

In five minutes, Benjamin shared his thoughts on regulation, huckster ICO's and the potential of blockchain.

WE ARE HERE WITH YOBIE BENJAMIN. COULD YOU INTRODUCE YOURSELF TO OUR AUDIENCE AND TELL THEM WHAT YOU'RE DOING RIGHT NOW?

Hello, my name is Yobie Benjamin and I am the current CTO Emeritus of Token.io, which is a distributed ledger company built to support the banking industry. If there's a really easy way to explain it, it's a far more modern version of SWIFT, which is the global bank system wherein money is moved.

YOU HAVE A BIT OF A DIFFERENT OPINION ON GOVERNMENT REGULATIONS FROM WHAT I UNDERSTAND. COULD YOU TALK A LITTLE BIT ABOUT THAT?

I am, believe it or not, quite a fan of government regulation. By background I was the former global CEO of Citigroup.

I currently sit on the Federal Reserve faster payment task force. So, my view on regulation is that regulation is good and regulation actually legitimizes a business. I'm not a big fan of an uber-libertarian movement, which says that regulation is bad and we don't need any of it, and the world is going to be perfect without any regulation.

CRYPTOCURRENCIES ARE HOPED BY SOME TO BE USED TO SORT OF DISRUPT THE SYSTEM AND TAKE EVERYTHING AND MAKE IT SOMETHING NEW. DAVOS IS NOT LIKE THAT. YOU SEE BLOCKCHAIN ALL OVER THE PLACE IN DAVOS. WHY DO YOU THINK THAT IS?

Interestingly enough, this is the first year in Davos that we have seen so many blockchain companies. Take the World Economic Forum (WEF), if you look at the formal program, it has probably about two hours of blockchain programming. The issues that concern the WEF are far more diverse and far deeper than blockchain itself. Blockchain is an important technology, clearly, probably, one of the most important technologies. But blockchain also has, basically, the way I would say, has given birth to many great technologies but also many hucksters. I think that is common knowledge in this industry – we see Blockchain companies, you know, selling things such as – unfortunately – prostitution. Or other types of things that are not really part and parcel of a global system and shouldn't be a part of the global system. I think blockchain does a lot in terms of global trade, doing trade finance, doing things that don't require high-velocity transactions or high-frequency transactions. But there is a lot you can do in blockchain. Municipal governments, property titles, you know, municipal fines – all sorts of records can be put in a blockchain. But not everything fits on the Blockchain. For example, when I was global CTO of Citibank, we did three to nine trln dollars of transactions a day. As you know, the blockchain itself in its totality, given all the crypto of Bitcoin and Ethereum, doesn't even come close to 1 trln dollars a day.

HOW SHOULD PEOPLE WHO ARE LOOKING AT A LEGITIMATE COMPANY OR ICO GO ABOUT THINKING THROUGH THEIR INVESTMENTS, COMING FROM YOUR PERSPECTIVE? HOW DO YOU SPOT THE HUCKSTER?

ook, here's what I see about [initial coin offerings (ICOs)], right? Right now, an ICO happens, somebody comes up with a great idea and then suddenly hires two developers, which becomes four developers, then they write on the ERC20 protocol and they have an ICO. Essentially short-circuiting what it's been a long formal process of an initial public offering [IPO]. In a lot of ways that's good, because it expands access to capital. However, it doesn't give an excuse for beginning to go and offer things to the market, that border on silly, if not criminal.

I think that if you're looking for an ICO and you think you want to invest in an ICO look at the team, this is a pretty standard piece of advice. But look if they're open to getting themselves registered. Many companies are doing ICOs that are not afraid of the registration process. Many companies are not afraid of regulation. They fully put themselves in front of regulators and make themselves available to questions and make themselves available to criticism much like any other IPO process. I personally like ICOs. But, given that there are probably thousands if not tens of thousands of ICOs that are forthcoming, it's a buyer beware market. That's all I can say for that!

> ***Blockchain does a lot in terms of global trade – doing trade finance, doing things that don't require high velocity or high frequency transactions.***

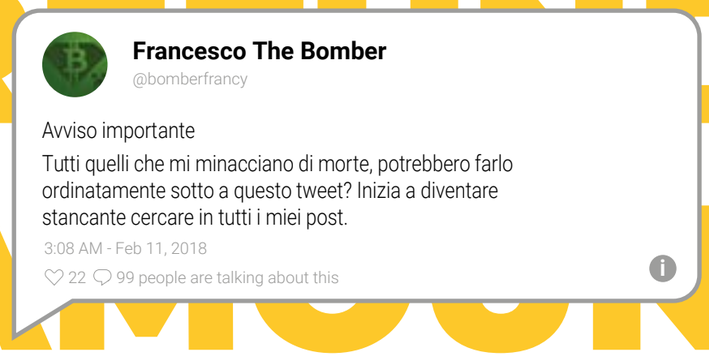
IT'S IMPOSSIBLE TO REFUND THE STOLEN AMOUNT

INTERVIEW WITH BITGRAIL'S FRANCESCO FIRANO

Cointelegraph talked to Francesco Firano, CEO of Bitgrail, the Italian exchange hit by a cyber attack that has caused the loss of a considerable amount of Nano tokens, formerly known as Raiblocks.

BitGrail froze trading on Feb. 8. The exchange stated that 17 mln Nano had been stolen in the hack, an amount worth about $187 mln at the time the losses were discovered.

The statements of the developers of Nano on the matter, mixed with the understandable anger of the users affected by the theft and the dissemination of confusing information, have generated a climate of strong hostility towards BitGrail's team. The hostility then escalated to serious threats and intimidating messages.



"All those who threaten me with death, could they do it neatly under this tweet? It starts to get tiresome looking in all my posts,"

Francesco The Bomber (@bomberfrancy) 11 February 2018.

On Feb. 13, the BitGrail team published an update on their website about the status of the investigations. The statement reads:

> *"We reiterate that we have filed a regular complaint to the competent authorities reporting the information regarding the hacks and the exploited bugs (not attributable to our software)."*

BitGrail explained that during communications with the developers of Nano, they have not managed to create a good dialogue.

> *"We have filed a further complaint about aggravated defamation in the press (as the newspapers all over the world have reported their defamatory statements) against the developers of Nano."*

HOW DOES THE BITGRAIL TEAM RESPOND TO ALLEGATIONS THAT IT TRIED TO COVER UP THE THEFT THROUGH REQUESTS TO THE NANO TEAM?

We, unlike [the Nano team], have nothing to hide. We are not forced to defame and make accusations without evidence. I can see they're very stressed by this matter.

WHAT PROGRESS ARE YOU MAKING TOWARDS THE RESOLUTION OF THIS MATTER??

First of all, we are trying to understand how to proceed from a legal standpoint. Once we understand what we can and cannot do legally, we'll proceed.

HOW WOULD YOU COMMENT ON THE REACTION FROM THE INTERNATIONAL COMMUNITY ON THIS MATTER?

No comment, it comments itself.

HAVE YOU PLANNED A POSSIBLE SOLUTION ALREADY FOR THE FUNDS LOST BY YOUR CUSTOMERS?

When it's ready, we'll communicate it to our customers.

DO YOU EXPECT TO FIND A REFUND SOLUTION FOR THE CUSTOMERS, EVEN IF THE NANO TEAM DECIDES NOT TO COOPERATE?

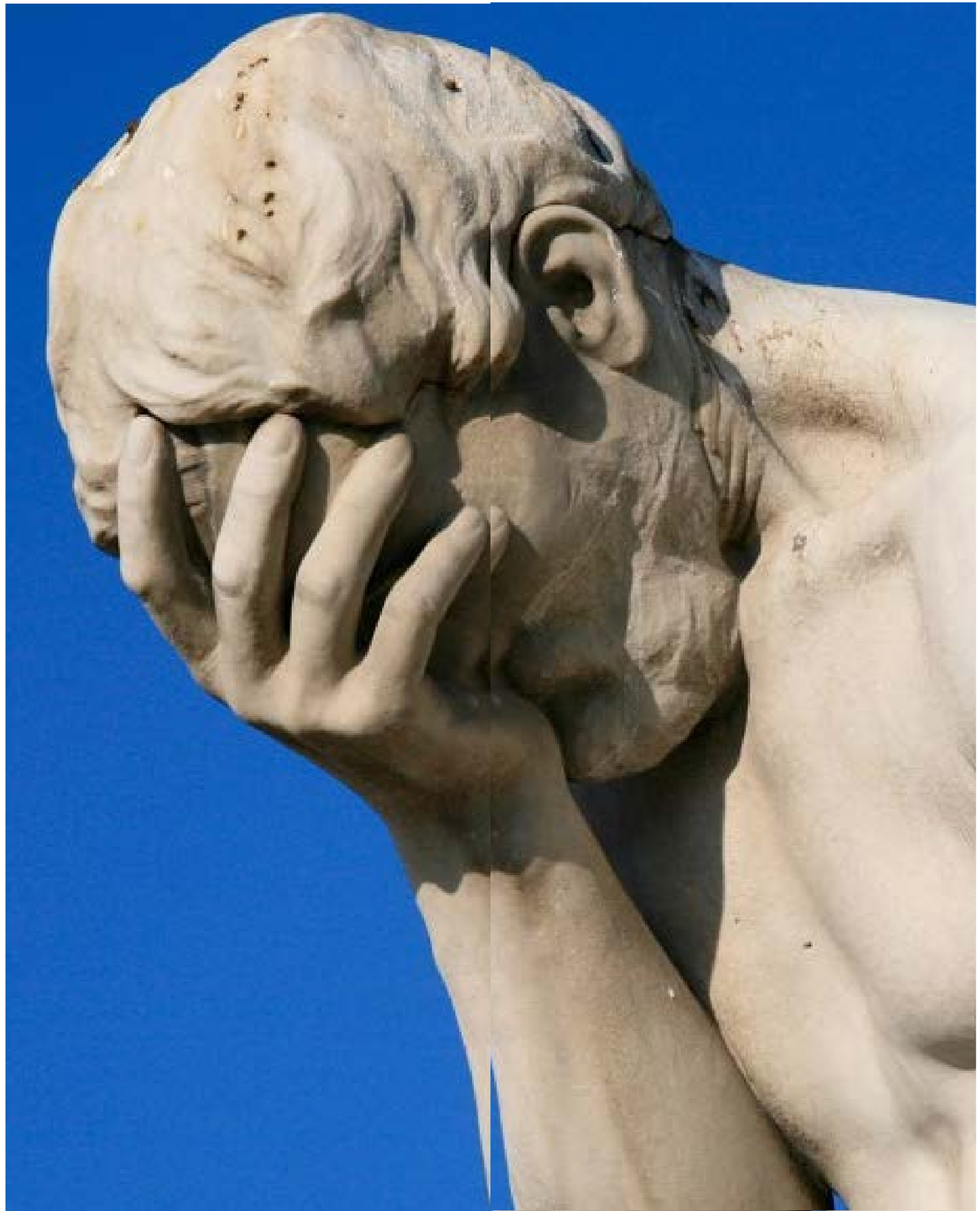
No, it's impossible to refund the stolen amount.

WE LEARNED THAT SOMEONE PUBLISHED YOUR PERSONAL HOME ADDRESS ONLINE. CAN YOU CONFIRM THIS ACTUALLY HAPPENED? HAVE YOU BEEN THREATENED?

Threats and addresses are in plain sight by now in my posts everywhere.

SOME MEMBERS OF THE COMMUNITY ASKED IF YOUR TEAM ALREADY KNEW ABOUT THE SECURITY FLAW AND IF YOU WERE WORKING TO FIX IT. WHAT WOULD YOU SAY TO THESE USERS?

Baseless and malicious accusations are done by the Nano dev team. The truth is their block explorer is dated Jan. 19, the date of the theft. Since RaiBlocks have no timestamps on the chain, we cannot really find out when it actually happened other than rely on the block explorer, which, as already shown by the private conversation they disclosed, is totally unreliable.



WHY DID YOU ASK THE NANO TEAM FOR LEDGED MODIFICATION?

I'll report an extract of the chat that the Nano team disclosed without authorization.

> "THE BOMBER, [08.02.18 19:30]
>
> Are we thinking about how we can solve this situation? One solution can be, I give you BitGrail with all wallets and db, and you fork the burned transaction to refund users. The alternative is that this money is probably lost forever. Guys, I understand it's a shock to everyone, but we must try to solve the problem and communicate something to users. As you can see, our only intention is to refund the users who took some serious damage."

As the conversation shows, I proposed to take a step back and let them manage the entire exchange until the resolution of the problem.

Instead, the dev team started to spread statements where they accused me of wanting to cover up the whole thing.

IN SOME POSTS, USERS SAY THAT THE TRANSFER OF NANO MAY HAVE STARTED WAY BEFORE YOUR ANNOUNCEMENT. WHAT WOULD YOU SAY TO THESE USERS?

Firstly, they don't have the complete data, as it is only available to us and law enforcement authorities. Secondly, we cannot rely on the official explorer developed and managed by the Nano dev, as it has been proved flawed – and which is, to this day, the only way to determine the date of the transactions.

TOP UNIVERSITIES PROVIDING BLOCKCHAIN COURSES

A NEW SUPPLY FOR A NEW DEMAND

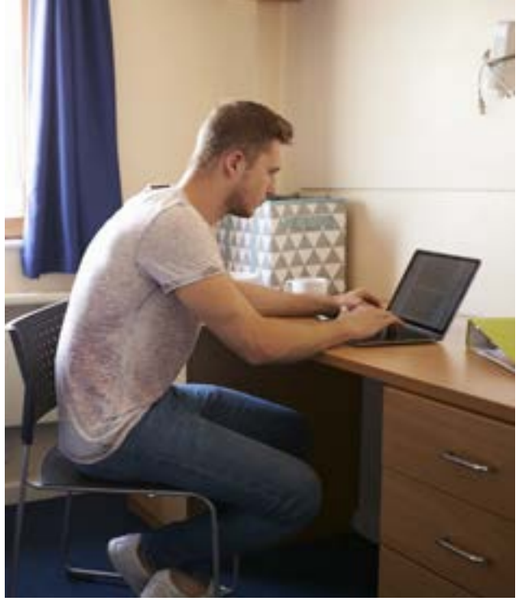
As the market cap for cryptocurrencies grows each day, it becomes harder and harder for the world to ignore this burgeoning market. The financial industry currently has a large demand for blockchain specialists and cryptocurrency experts. The only problem is that there is not a large enough supply of workers to meet that demand.

Why the insufficient supply?

Bitcoin was launched in January 2009. The cryptocurrency is not even ten years old yet – so it's not too surprising to learn that many people are unaware of blockchain technology and its benefits, which explains why the supply of blockchain and cryptocurrency specialists does not currently match the demand.

To combat this, universities around the world have been implementing blockchain and cryptocurrency-related courses and clubs to adequately prepare their students for jobs in an industry that will define the future of banking and finance.

In the US, universities such as NYU Law, Duke, Princeton, Stanford, and UC Berkeley are just a few among the many schools implementing such courses. Some of the titles of these courses are Digital Currency, Blockchains and the Future of Financial Services (NYU Law), Bitcoin and Cryptocurrency Technologies (Princeton), and Cryptocurrencies, Blockchains, and Smart Contracts (Stanford).



In Europe, the University of Cumbria, B9 Lab Academy, IT University of Copenhagen, and University of Nicosia are just a few of the higher-learning institutions that have implemented such courses. In Russia, the Moscow State University of Economics, National University of Science and Technology, and Moscow Institute of Physics and Technology have done the same.

Crypto becoming so widespread that it is not only attracting the attention of scholars, but also students who have taken an interest in the future of money and banking. These students have been launching their own initiatives to make their peers aware of what the future of monetary transactions will be.

Derek Strauss, a junior at Florida State University (FSU), is currently in the process of establishing a cryptocurrency club at FSU. Strauss said how he made the decision to create a cryptocurrency club:

> ***"I went onto our school's organization website and realized nothing existed. After discovering there currently wasn't anything, it inspired me to create a club to share my passion of cryptocurrency with other students. I wanted a place where I could help other students learn about an emerging industry and the technology behind it."***

Similar to Strauss, there are many students taking initiative to spread knowledge that will be essential to the future of transactions. The Blockchain Education Network has been partnering with students who've created blockchain/cryptocurrency related clubs and groups for quite some time.quite some time now.

What prompted the spike in demand?

In 2007 and 2008, it was believed that banks were too big to fail. In 2009 we learned that belief was horseradish. Financial institutions around the world are realizing that the future of money is not fiat. Fiat was great – in the late 1700's when Alexander Hamilton proposed that America needed a replacement for money in the form of coins – but it's now 2018 and fiat has become inefficient and outdated. Similar to when your office decided to go paperless when Earth's environment issues became a concern, soon, financial institutions will be going paperless (fiat-less), to make transactions in this world more efficient and cost effective. To accomplish this, these institutions know it is necessary for them to have a blockchain team, and you can't have a blockchain team unless you have a group of people who are knowledgeable or have been properly educated on the matter.

What does this mean for the future?

When Cointelegraph asked Strauss what he believed the future of cryptocurrency to be, he replied, "I foresee a shift [from fiat] in the future. [I think] people [will be] using cryptocurrency to purchase goods and services. Companies such as Overstock have already been accepting Bitcoin for a number of years now. While I do believe cryptocurrency will eventually be used as a means for payments, I think in the short term we will see the implementation of blockchain technologies. Considering that IBM and Microsoft have been implementing blockchain into their companies, you have to take note that other major corporations will be likely to follow so they are not left behind."

No institution wants to be left in the dust due to one of their competitors, and that is why more and more financial institutions are looking to hire a blockchain team. That is why more and more universities around the world are implementing blockchain and cryptocurrency related courses, clubs, and groups.

In 2007 and 2008, banks were "too big to fail" – in 2009 America learned that was not true. In 2018, Cryptocurrency is too big to continue to be ignored, and everyday the world continues to learn just how true that is.

LUMI

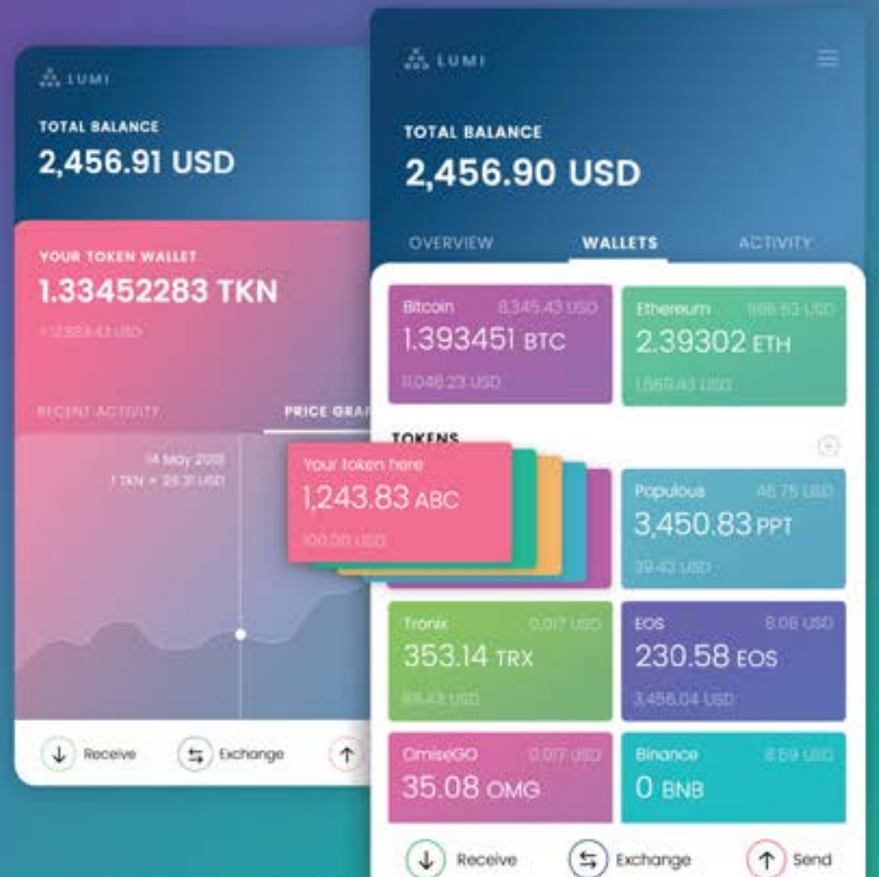
We at Lumi Technologies have a vast experience in creating and customizing crypto wallets

Token listing

We add your token card to our wallet. The token will be available for all users and token holders to send & receive. The price graph is included in the card.

White label wallet

We create a crypto wallet for you in quite a short time period. We offer a variety of options so that you can get a perfectly customized wallet that meets your needs.



Bitcoin
Bitcoin Cash
Ethereum
tokens ERC 20
tokens ERC 721
and more coming
+ exchange

iOS

Android

Desktop

lumiwallet.com

Pssst!
Need a cool wallet
for your business?

up to
-70%

Use the wuf promo code to get a discount for any crypto wallet solution

We just like dogs, that's why there is a huge dog

lumiwallet.com
hello@lumiwallet.com

Download on the App Store

GET IT ON Google Play

THE VIEW FROM THE OUTSIDE

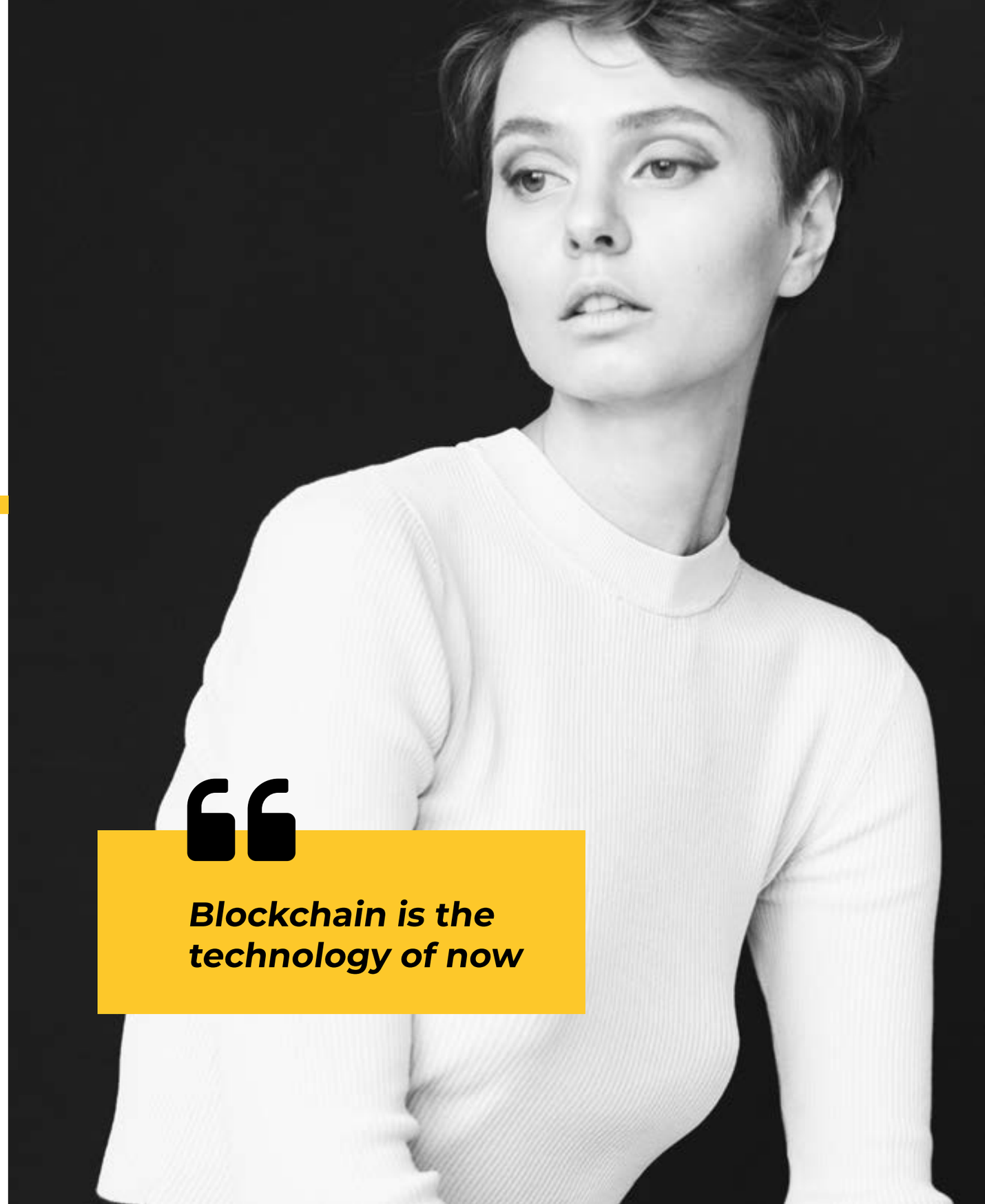
A NEW GENE IN BLOCKCHAIN'S DNA

One can compare today's blockchain technology – which will no doubt continue developing – with Windows 3.1. It's almost impossible to look at it without crying. The most significant breakthrough in Internet technology is also a pimpled geek.

The blockchain needs a new gene pool. This gene pool should be as different as possible from the existing one to produce worthy offspring. Just think, an expanding gene pool can force a shark to swim to the other end of the world to procreate.

There is a market that inhabits a world so different from blockchain that even the wildest of fantasies wouldn't pair them together: the fashion modeling market.

Cointelegraph talked to a former model, Anneliya Garifulina, not just for the sake of an attractive photoshoot in the magazine, but to show that blockchain and modeling share common ground.



ANNELIYA

A former model, economist, blockchain ambassador and TV host from Taipei talks about Chinese mentality and reflects on the future of the cryptoworld.

Anneliya Garifulina moved to Moscow from Taipei two years ago, after having worked on Taiwanese TV and obtaining a sizeable army of fans. Hanging out with friends who work in the IT industry, she has been familiar with the world of cryptocurrencies as far back as 2011.

Furthermore, she is employed as a blockchain ambassador at Botanico.co, the crypto first modeling agency providing the environment for women to integrate themselves with the crypto community. Botanico.co also hires out models for ads and promotional campains. This will help to draw attention to the project making the blockchain industry more vivid.

Today, Cointelegraph spoke with Anneliya Garifulina about blockchain and what it has to do with modeling.

WHAT WAS YOUR FIRST REACTION AFTER BECOMING A BLOCKCHAIN AMBASSADOR?

When Botanico asked me to join the Blockchain Ambassadors, I was impressed with the bold idea of making the geekiest sphere beautiful. To be honest I do think IT is sexy, and of course I agreed to participate. I thought that now I am in the area on everyone's lips – that's pretty cool too.

WHAT DID YOU DO IN TAIWAN? WE KNOW YOU WORKED THERE FOR QUITE A WHILE.

The first time I visited Taiwan, I fell in love with the country and the culture. At some point, I decided to move and stayed there for five years. I started learning Chinese and managed to start speaking it after two months of studying.

IS IT REQUIRED FOR A MODEL WORKING IN TAIPEI TO LEARN CHINESE?

Not really. But I was a featured guest on a Taiwanese talk show for students, so I had to speak to draw attention to my personality. It worked out because I got quite popular on Facebook.

YOUR EXPERIENCE SEEMS EXTRAORDINARY, BUT HOW ON EARTH DID YOU GET INTERESTED IN BLOCKCHAIN?

I personally google pretty much everything because I am curious. Technology never scared me and I never had trouble, let's say, setting up a router by myself. I got familiar with Bitcoin back in 2011.

Photo: Anisia Kuzmina

> ***The possibilities for Blockchain are endless.***

WHO INTRODUCED YOU TO THE CRYPTO INDUSTRY?

I have many friends who work in the IT industry, and I am pretty sure I first heard the term Blockchain from them when it was not as spread-out as now.

WHAT IS YOUR PERSONAL UNDERSTANDING OF BLOCKCHAIN?

I know that it helps with transactions and operates as a set of blocks with data. But from what I see in the media, the possibilities for Blockchain are endless and it can influence almost any businesses. My friends and I want to believe this innovation will make the world better soon.

BOTANICO HELPS MODELS INTRODUCE THEMSELVES TO THE BLOCKCHAIN INDUSTRY. HOW DO YOU THINK BLOCKCHAIN AMBASSADORS THEMSELVES CAN HELP THE INDUSTRY IN RETURN?

It's a legit idea. Beautiful faces are needed for blockchain and the models are happy to help. But what's more important this industry must have a human face, people should not be scared of the complexity of blockchain. I want them to look at me and think: "Well, if she understands it, I can understand it too."

THE SABER CASE:

HOW COMPLEMENTARY CURRENCIES CAN GO CRYPTO AND CHANGE THE WORLD

In the past few years we've been witnessing the massive waves of cryptocurrency adoption – you can now pay in Bitcoin for almost anything from coffee to real estate. However, the ideas were always above money in community and there is still so much untapped potential from decentralized digital coins.

A history of Saber – a Brazilian complementary currency project, developed in the early 2000s to promote the educational system, is an important example of the social potential we tend to forget by keeping up with the rates of exchange.

Brief history of complementary currencies

Complementary currencies (CCs), also known as community currencies, are basically an alternative, or indeed a compliment, to conventional money. Their purpose is usually to strengthen the local economy at times of recession by stimulating additional transactions and therefore keeping the economic cycle in motion or to achieve certain social, environmental, or political goals.

In most cases CCs are not legal tender – i.e. they are not accepted at a national level and you can't buy whatever you want using it – they only function as a quasi-monetary exchange medium for certain purposes within a restricted area. In theory, CCs should stimulate the local economy and encourage people to act collectively. Although replacing conventional money and undermining national currency is not usually the goal of a CC, the state often appears to be reluctant to the idea, and the model has developed the reputation of an experiment and not a proven method.

The first CCs can be traced back to ancient Egypt, where local people used otrakas – pieces of pottery – to issue receipts for the amount of harvest farmers would put into storage. Those pieces, in turn, were traded for local services. Similarly, in medieval Europe people would regularly turn in bracteates – pieces of jewelry – for new coins, although always with a deduction. The system was designed to prevent people from hoarding coins and keeping them out of the financial ecosystem. That, in turn, would increase the velocity of regular money.

In recent history, CCs started to appear in the first half of the 20th century. One of the most notable example is the Wära free economy experiment held in Germany. The Wära was a currency introduced by Hans Timm and Helmut Rödiger, followers of Silvio Gesell, a German merchant, theoretical economist and anarchist. During the course of the experiment, Wära banknotes were printed and were made available in denominations of 1/2, 1, 2, 5, and 10 Wära. One Wära would be equal to one Reichsmark, and the aim of the Wära was to support the economy of a mining town Schwanenkirchen, which had been hit with massive unemployment. Like otrakas in Ancient Egypt and bracteates in medieval Europe, the Wära was a demurrage-charged currency, which means that each banknote had a monthly cost fee of one percent of its nominal value. This prevented the people of Schwanenkirchen from storing the currency and putting it out of active circulation. It had its benefits for users too: for example, people who bought coal – the local economy's staple – using Wära received a discount.

During the course of the experiment, the Wära allowed local services to continue despite the fact that the national currency was scarce. As a result, new jobs were created and taxes were paid. However, the scheme ended abruptly: the finance ministry of the Reich forbade the currency, and the town returned to its previous decadent state.

Similar experiments were held in other countries around that time: local currencies were used in Wörgl, Australia (1932 – 1934), Alberta, Canada (1936) and in the US during times of the Great Depression.

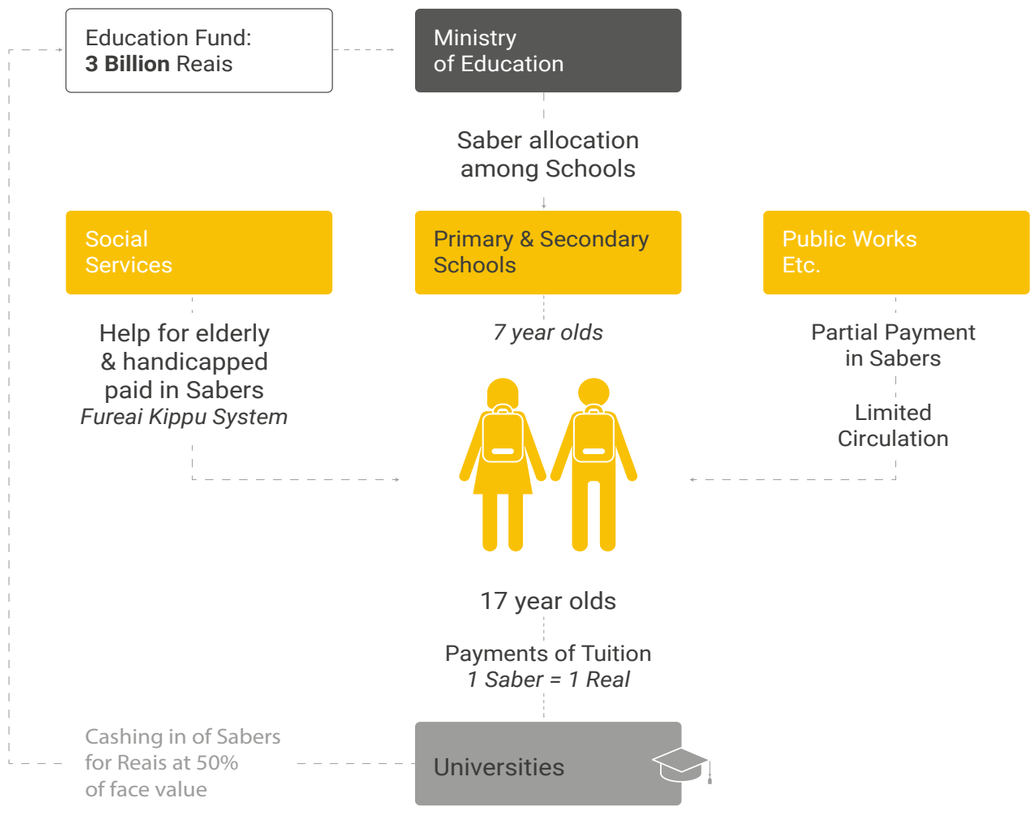
The Saber Experiment

In 2003 Belgian economist Bernard Lietaer collaborated with Brazilian professor Gillian Schwartz of São Paulo University – who has previously worked as an economist at various public and private financial institutions including BankBoston – to submit a proposal for a complementary currency called the Saber to the government of Brazil.

Saber was aimed to help Brazilian schools provide greater educational opportunities "without creating any new financial pressure on the economy". The educational vouchers were designed to launch a substantial "learning multiplier" so that a given amount of money can produce more learning for a bigger number of students. In other words, the Brazilian Ministry of Education would allocate Sabers among schools in economic areas where normally there is no funding for higher education. Local students at the age of 7 were to receive a certain amount of Sabers on the condition that they must choose a mentor among older students. They can later earn more Sabers by giving those lessons at the rate of 5 Sabers per hour. At the end of the program, when they turn 17 and graduate from school, they could spend the gathered Sabers to pay – whether fully or partly depending on the available amount – university tuition fees.

SABER COMPLEMENTARY CURRENCY SYSTEM

LEARNING MULTIPLIER



The mere idea of an alternative to the national currency sounded rather controversial. As Schwartz remembers over a Skype call with Cointelegraph:

> *"Pioneers are doomed to see the other side of Jordan river, but never make it there. Maybe I was researching [the concept of CCs] too early, but anyway it's not about anyone's idea, it's more about the zeitgeist".*

The Brazilian government declined the project at the review stage. However, 18 years since Schwartz's team first started doing research on CCs, things have changed considerably. Now, the rise of Bitcoin allows more room for experiments in the financial area. Schwartz noted:

> *"I think it's a learning process for everyone. Now the private banks, as well as some departments at a federal level are discussing blockchain technology here. São Paulo's stock exchange has also been one of the pioneering institutions [in that regard].*
>
> *Now it's becoming much easier to explain to my partners, local leaders or young people what a creative currency could be, because there's Bitcoin and all that discussion whereas 10 15 years ago that would be seen as completely out of the question – [the response would have been] how can you even dare to substitute the real currency?"*

What's next?

A global creative cryptocurrency to promote education, culture and arts worldwide

These days Schwartz is busy creating a CC that goes beyond the regional – the project was launched in Brazil in November 2017, although at its most initial stage. "We lack a monetization platform for creative processes which already exist [in our society]. [The world] should be more democratic rather than autocratic and technocratic" – he says, while stressing the popularity of state-reinforcing technologies like mass surveillance in modern society as well as fluid stability of global currencies over the past few decades.

> *"We're working on the idea that we can share digital toolkits that may include the creative currency. It's a concrete example of this idea of a great creative community that is leveraged by universities, artists, citizens into a whole new sphere for information exchange and local development. Whilst it doesn't involve governments, it's not against governments."*

Why not issue a new coin straight away, when it seems so easy to do in a world where even memes almost accidentally become successful currencies? Well, according to Schwartz, it contradicts the whole idea. “It makes no sense to go for an initial coin offering (ICO) if you don’t have the other ICO, which is Initial Community Organization. You need [to establish an] organic connection between community and the currency first. The idea is not that we want hundreds of new ICOs, we’re aiming at a currency system with diversity being an important part of its dynamics. It’s really complementary, it’s not antagonistic to the existing currencies and infrastructures. We’re not going backwards in terms of globalization – that’s for trade barriers advocates. Instead, we’re going forward, towards more interconnectivity but with a balance between the technological and the humanitarian”.

Acknowledging that conservative governments of the world would not be particularly happy about the idea that a regular, state-approved currency can be in any form substituted by decentralized ones, Schwartz seeks support among more open-minded institutes: universities, research groups and outreach projects.

“So far, we haven’t leveraged enough support… there’s a funding issue here” admits Schwartz. “In order to develop something like a running currency, confidence is required. To get that confidence, you have to be trustable as an institutional body or as an organization. We still haven’t been able to convince any policymaker." However, DarVoz has found an alternative solution: these days Schwartz and his team are discussing their concept with other universities all around the world: "That way, we should be able to have a global social currency that connects different cultural and educational projects”.

Crypto technologies and transparency

To run such currency, DarVoz needs a platform. Schwartz’s team is currently negotiating with Holochain, an open source framework for peer-to-peer applications. “We’re going to hold a meet up with their team to brainstorm at the end of March. [But the] political situation in Brazil is very unstable at this point. In the 21 years that I’ve been working with those projects at University of São Paulo, this is the worst time to start” the professor laughs. Some caution wouldn’t hurt, Schwartz believes:

> *“It’s important to hold an open dialogue with the central bank as to what kind of currency that is and what kind of sphere it’s connected to… all kinds of walls are being built these days. It’s kind of like going back to the middle ages in that sense”.*

The currency’s purpose is part of its value, as opposed to regular currency, which, according to Schwartz, “is useful for whatever – [with regular money] you can buy a gun, you can buy a glass of water”. His team is looking to achieve NGO levels of transparency – the activities circulating within the currency must be traceable and accountable for in order to be monetized. Such digital records are supposed to be stored within the blockchain-type backbone of the currency:

> *“It naturally evolves into the public sphere of shared audiovisual content… Say, you held a lesson with 15 kids in Bolivia and took care of the garden around the church. You connect to the global network and share the record of your activities… Basically, it’s about how you translate knowledge into acknowledgment on a democratic [platform]”.*

Despite the complexity of his concept and low interest among policy-makers and investors, Schwartz remains optimistic. “This is a learning process. The issue here is not about the currencies, it’s about all countries reaching a new level of understanding that can be at least comparable to the post-war welfare consensus. We’re now probably living through the last stages of the crisis. A new consensus is very likely, because we have much more tools to discuss, share and use. However, on the other hand, those very tools are very useful for control, censorship and oppression as well. You can use a knife to kill or to slice the bread and share.”

A GLIMPSE INTO THE FUTURE

WHAT HAPPENS WHEN THERE ARE NO MORE BITCOIN TO MINE?

Bitcoin's (BTC) blockchain hit a unique milestone in April 2018 as the 17 millionth BTC was mined.

If you're wondering why this number is significant, it's because there are only four mln tokens left to mine before the 21 mln BTC cap is reached. However, the truth is that most people alive today are unlikely to see that happen.

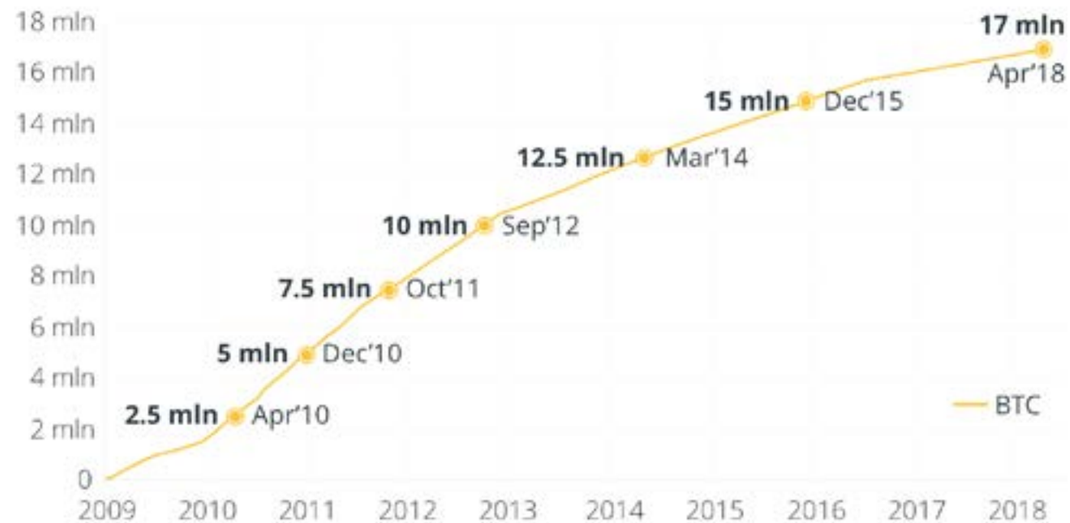
Bitcoin's blockchain protocol makes mining more difficult as more miners join the pool, and the Bitcoin reward for mining a block also halves every 210,000 blocks. As it stands, miners receive a 12.5 BTC reward for unlocking a new block. According to BitcoinBlockHalf.com, the next reward halving will happen in May 2020 – reducing the reward to 6.25 BTC.

Assuming that there are no changes to the protocol, the Bitcoin cap will be reached by 2140, 122 years from now.

Nevertheless, it's taken just 9 years to mine 80 percent of the total Bitcoin that will ever be available – a little over 520,000 blocks, as shown in the graph on the following page.

The next reward halving will happen in May 2020

BITCOINS IN CIRCULATION



BLOCKCHAIN SIZE

What happens when we mine the last Bitcoin?

Currently, miners are still heavily incentivized to mine in order to obtain increasingly more valuable Bitcoin tokens as a reward before the supply reaches its capacity.

However when the day comes that the 21 mln cap is hit, there will be no more BTC rewards for miners. However, transactions still need to be validated and stored on blocks in the blockchain – so miners will only benefit from transaction fees.

As it stands, Bitcoin transactions are processed by the network in order of the transaction fee associated to that specific transaction. The higher the fee, the more incentive there is for a miner to prioritize your to be included in a block.

This could essentially be the lifeblood of miners in the next century once there are no more BTC tokens to be unlocked. This is laid out in Satoshi Nakamoto's Bitcoin whitepaper:

> ***"Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free."***

What could happen in between?

A major point to consider here is that there are more than 100 years to go before the last Bitcoin is created. Considering that it's just been short of 10 years since the Bitcoin's inception, a lot could happen during this time.

As Nakamoto envisaged, nodes are responsible for maintaining the Blockchain and verifying transactions. The move away from a trust-based system to a proof-of-work system that operates by consensus of the longest chain:

> ***"They [nodes] vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism."***

The last sentence of that statement is particularly telling, as miners and exchanges have had to operate in tandem at trying times in the last few years.

Segwit revisited

In 2017, the issue of scalability, block capacity and transaction costs came to a head. In 2010, Nakamoto implemented a 1MB size limit for blocks in order to stop miners from producing bigger blocks that were likely to be rejected by the network – which could have caused the Blockchain to split.

At the time, the limit was big enough due to the small amount of transactions and the fact that a change could be implemented at a later stage – if need be. Nevertheless, Bitcoin Core developers eventually came up with a solution known as Segregated Witness, also known as SegWit. In essence, SegWit separates non-signature data from signature data of each transaction, reducing transaction sizes stored on a block. Furthermore, it cancels out transaction malleability by removing signatures from transaction data – which paves the way for lightning network integration.

SegWit was implemented in Aug.2017, as major stakeholders and Bitcoin companies pushed for a solution to high transactions fees caused by a backlog due to the block size limit. Some called for bolder measures – an increase in the block size to 2MB called SegWit2X. There were a number of issues, namely the lack of replay protection and the fact that the move would require a hard fork. Ultimately the change was never implemented. The implementation of SegWit was possible due to the consensus of the Bitcoin community – just as Nakamoto pointed out in his white paper. Where there were greater concerns, the community was divided and the change was never implemented.

Changes to the protocol

Segwit's implementation has been slow across the overall network since August 2017. Big players like Coinbase and Bitfinex only introduced the change in February 2018.

The launch coincided with lowering transaction fees – a testament to the intended outcome of Segwit integration. As the following graph shows, transaction fees have dropped considerably in the past few months as Segwit continues to be implemented to nodes around the world.

Lightning network

SegWit's implementation also laid the foundation for second layer solutions to further improve Bitcoin's network.

The most anticipated is the Lightning Network, which will essentially do what SegWit has done but on a grander scale.

In layman's terms, the Lightning Network will allow users to open up multiple payment channels between themselves off the Bitcoin blockchain. The channel will be opened and recorded on the blockchain, but transactions will be done off chain until the payment channel is closed.

In essence, users deposit Bitcoin into this channel and make transactions by transferring promise of ownership to each other. When they decide to close the channel, the users take their proportion of the total sum and the ownership of those amounts is recorded on the Blockchain.

To get an in-depth explanation, you can read Cointelegraph's Lightning Network guide.

What matters here is that this second layer solution will greatly increase the speed of transactions and therefore the network as a whole.

However, this does pose some interesting questions for miners in the future. Once all 21 mln Bitcoin have been mined, transaction fees will be the only incentive for miners. If the Lightning Network is full integrated by this time, there could be far less transactions being recorded on a daily basis. This could potentially affect the amount of money miners will be making from transactions.

However, 100 years from now, it seems likely that all of these problems will have been answered by Bitcoin Core developers and the wider cryptocurrency community.

TOP PEOPLE IN BLOCKCHAIN

top.cointelegraph.com

Co-founder of Ethereum

Vitalik Buterin

@VitalikButerin

The genius behind the world's second most valuable cryptocurrency today – Ethereum – first learned about cryptocurrencies from his father. After co-founding Bitcoin Magazine in 2011, Buterin spent two years learning Blockchain technology, its potential, and the applications it had to offer. The Ethereum white paper was published in late 2013. Buterin currently serves as the Chief Scientist of the Ethereum Foundation and leads Ethereum's research team, which maintains the core technology of the cryptocurrency and works on future versions of the Ethereum protocol.

Bitcoin Evangelist & Author of 'Mastering Bitcoin'

Andreas M. Antonopoulos

@aantonop

One of the world's greatest advocates of Bitcoin, Blockchain technology, and the principles of decentralization, Antonopoulos is a security and distributed systems expert, a widely published author of books, articles, and blog posts on cryptocurrencies, a frequent speaker at technology and security conferences worldwide, a coder, and an entrepreneur. Antonopoulos offers strategic consulting to a small number of cryptocurrency companies, as well as offering expert witness testimony as an expert in the security, technical details and use of cryptocurrencies.

Creator of Litecoin

Charlie Lee

@SatoshiLite

Primarily known in the crypto world as the creator of Litecoin, Lee – like many early adopters of Bitcoin – entered the crypto sphere by getting into Bitcoin mining. Lee sees Litecoin as the cryptocurrency best suited for smaller, lightweight transactions like online retail shopping, while Bitcoin is the currency for more heavyweight transactions like international payments.

Creator & Designer of Bit Gold

Nick Szabo

@NickSzabo4

A major influencer in Bitcoin, Szabo's expertise with cryptocurrency started back in 1998 with the creation of the BitGold proposal, the predecessor of Bitcoin. People have speculated that Szabo is Satoshi Nakamoto, the anonymous creator of Bitcoin, although Szabo has repeatedly denied the claim. Szabo is still considered the 'father' of 'smart contracts,' a term usually associated with Ethereum, and he continues to contribute his technical knowledge and commentary in the crypto industry.

Co-founder of Blockchain Capital

Brock Pierce

@brockpierce

As an early investor in Bitcoin, Pierce is a venture capitalist and entrepreneur with an extensive track record of founding, advising and investing in disruptive businesses. He pioneered the market for digital currency in games, and was one of the largest investors in the Ethereum crowdsale. Pierce has invested in over 30 companies in the Blockchain ecosystem, participated in over 100 projects, and helped raise over $200 million US for companies he was involved in. Pierce has also been a guest lecturer at the Milken Global Conference, Singularity University, Stanford University, the University of Southern California, and the University of California, Los Angeles.

President & CEO of The Tapscott Group, Inc.

Don Tapscott

@dtapscott

Tapscott has become an increasingly well-known figure in the cryptocurrency industry, having been one of the foremost authorities on the impact of technology for decades. He is also one of the most influential living theorists about business and society. Tapscott was identified as the most influential management thinker in the world by Thinkers50 and Forbes. He is the author or co-author of 15 widely read books about new technologies and new media in business and society, including 'Wikinomics' (2006) and 'The Digital Economy' (1995). His book, 'Blockchain Revolution' (2014), has made him one of the most active Blockchain governance references and proponents.

Senior Editor at Forbes &
Co-lead Reporter of the Forbes Fintech

Laura Shin

@laurashin

Shin is best known for her work as senior editor of Forbes' cryptocurrency and Blockchain coverage. She is also the host of the publication's Blockchain-focused podcast – Unchained – and authored the Forbes e-book, "The Millennial Game Plan: Career And Money Secrets To Succeed In Today's World" (2014). Her active participation in the crypto industry and her expert knowledges in this sphere make her one of the most influential persons in the crypto world.

Co-founder & CEO of Coinbase

Brian Armstrong

@brian_armstrong

With his double major in Computer Sciences and Economics, Armstrong had spent the most part of his life actively pursuing a career in the tech industry. Being well equipped for a foray into the tech startup arena, Armstrong co-founded crypto wallet and exchange Coinbase in July 2011. Coinbase was envisioned as a Bitcoin marketplace that would enable people to purchase the cryptocurrency more easily. Throughout his life, Armstrong has maintained a strong interest in the technology market and has always participated actively in developing solutions for the industry, becoming the leading advocate of Bitcoin adoption, as well as regularly speaking at conferences, workshops, and seminars. He was named "The Rockstar" in the Bitcoin community.

Founder & CEO of Digital Currency Group

Barry E. Silbert

@barrysilbert

Known as a founder of The Digital Currency Group, Silbert is a serial crypto investor and a well-known proponent of the rival Ethereum chain, Ethereum Classic. He is a frequent speaker at conferences on the topic of trading illiquid assets and has appeared in many leading publications, including The Wall Street Journal, Financial Times, New York Times, USA Today, BusinessWeek, Forbes, Fortune, and many others. In 2013, he started as an angel investor in Bitcoin companies, and he currently is one of the most influential figures and newsmakers in the crypto world industries.

Founder & CEO of ShapeShift.io

Erik T. Voorhees

@ErikVoorhees

Before he became an entrepreneur, Voorhees was a blogger with libertarian ideas, authoring long thoughts about the nature of money and politics and the role of cryptocurrencies in this balance. His active online presence ensures his voice is heard throughout both the crypto industry and mainstream media. Active in the industry almost since it began, Voorhees's greatest claim to fame is arguably his most successful project – the crypto exchange platform ShapeShift – and his well-known Bitcoin gambling game SatoshiDice.

Co-founder & CEO of CivicKey

Vinny Lingham

@VinnyLingham

Lingham's journey in Blockchain began with his startup Gyft, a service offering Amazon purchases using Bitcoin. He is a prominent commentator on Bitcoin and Blockchain, and is the recipient of numerous awards, including Top Young ICT Entrepreneur in Africa (2006) and Top 500 CEO's in the World by Richtopia (2015). Lingham was previously a finalist for Men's Health Best Man (2009) and ICT Personality of the Year in South Africa (2008). He is also named as one the world's great advisors.

Co-founder &
CEO of the Blockchain Research Institute

Alex Tapscott

@alextapscott

Tapscott is a prominent writer, speaker, investor and advisor interested in emerging new technologies, such as Blockchain and cryptocurrencies, and their influence on business, society, and government. He is the co-author (with his father Don Tapscott) of the critically acclaimed #1 Globe and Mail non-fiction best-seller, "Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money Business and the World" (2014), which has been translated into over 15 languages. Tapscott co-convened a meeting of Blockchain stakeholders to discuss the Blockchain ecosystem and he currently sits on the Advisory Board to Elections Canada. Tapscott has become a leading voice on cryptocurrency and Blockchain technologies.

Co-founder &
Director of Bitmain Technologies, Ltd.

Jihan Wu

@JihanWu

Wu is a Chinese entrepreneur, financial analyst, and Bitcoin evangelist. He is a major proponent of Bitcoin Cash, having previously supported Bitcoin network scaling solutions such as Bitcoin Unlimited. He believes that Bitcoin and Blockchain technologies are now significantly changing modern world and people's way of life. Wuis claimed to be one of the most controversial names in crypto industry meanwhile he is still one the most influential proponent of cryptocurrencies and Blockchain technologies worldwide.

Chief Scientist at Bitcoin Foundation &
Lead Developer of Bitcoin Core

Gavin Andresen

@gavinandresen

Andresen (formerly known as Gavin Bell) is a well-known figure in Bitcoin. A brilliant software engineer, he previously was a director and currently is Chief Scientist of the Bitcoin Foundation, as well as a Bitcoin Core developer. His technical involvement with Bitcoin stretches back to 2010, when he discovered Bitcoin, quickly recognising the benefits of its design. Andresen acts as arbiter and architect for the Bitcoin community and helps coordinate improvements to the core Bitcoin software used by the worldwide community.

Editor-in-chief at Adamant Research

Tuur Demeester

@TuurDemeester

Demeester is an independent investor, newsletter writer, and commentator. A globally-known entrepreneur and long-time cryptocurrency advocate, Demeester has maintained a heavy presence in Bitcoin and related debate online since 2013. Editor-in-chief at Adamant Research, he is well-known for his financial advice in the Blockchain industry. Before his career as an investment analyst, Demeester was actively involved in sudbury-type schools, a libertarian type of schools where students have complete responsibility for their own education, and Austrian economics.

Bitcoin Angel Investor & Bitcoin Evangelist

Roger K. Ver

@rogerkver

Ver is famous for being one of the first investors in the Blockchain industry, financing the growth of many of its biggest names. He runs popular news and wallet resource Bitcoin.com, and became a notable proponent of Bitcoin Cash in 2017. Ver is a legend in the Bitcoin community, named as the "Bitcoin Jesus" for his tireless evangelism of the virtual currency and for his investments in numerous Bitcoin startups. He called himself self-educated enthusiast who is spending his free time on studying economics and moral philosophy.

Co-founder of Netscape Communications &
Co-founder of LoudCloud

Marc L. Andreessen

@pmarca

Andreesen is a co-founder of Silicon Valley venture capital firm Andreessen Horowitz, contributing funding to multiple Blockchain industry startups since 2013. He has a background in revolutionary technology, co-creating Mosaic and Netscape, two of the Internet's first browsers. Andreesen is the recipient of numerous awards related to the Internet Industry, including Vanity Fair's 2011 New Establishment List, CNET's 2011 most influential investors list, the 2012 Forbes Midas List of Tech's Top Investors, and was one of five Internet and Web pioneers awarded the inaugural Queen Elizabeth Prize for Engineering in 2013. He was also named in the 2012 Time100, an annual list of the 100 most influential people in the world assembled by Time Magazine.

Co-founder & President of Blockstream

Adam Back

@adam3us

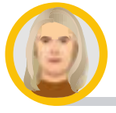
Back is a cryptographer and one of the founding fathers of 'Bitcoin-like' cryptocurrencies, developing Hashcash in 1997. He has become a major reference source in Bitcoin development, going on to co-found Blockchain tech company Blockstream in 2014. Back's work was one of the eight references Satoshi Nakamoto had in the original Bitcoin paper.

President of Crypto Valley Association &
Founder of Bussmann Advisory

Oliver T. Bussmann

@obussmann

Bussmann is a globally recognized technology thought leader and driver of large-scale transformation at multinational organizations. Bussmann is something of a banker-turned-Bitcoiner. He is the recipient of numerous awards, named COO/CTO of the year by Financial News/The Wall Street Journal, European CIO of the Year by INSEAD/CIONET, received the Elite 8 Award, which is given to the most innovative leaders in technology working in capital markets by Wall Street & Technology Magazine, and has twice been included on the Financial News "FinTech 40" list of innovators shaping the future of finance.



Director of Development
at Digital Currency Group

Meltem Demirors

@Melt_Dem

Demiros has a diverse background in management consulting, corporate treasury, commodities trading, and supply chain management. She calls herself a 'Blockchain believer'. As an experienced business leader, Demiros brings a wide range of international, multi-sector experience into building Digital Currency Group's global network. Her strategy is to focus on building and supporting Bitcoin and Blockchain companies by leveraging its insights, network, and access to capital.

Co-founder & CEO of Bloq

Jeff Garzik

@jgarzik

Garzik is one of the first Bitcoin Core developers. A futurist, entrepreneur and software engineer, he currently serves as the CEO of Blockchain-for-enterprise startup Bloq and remains a vocal commentator in the space on social media. He is also an advisor to several globally-known Blockchain industry companies, including Chain and BitFury.

Founder & Executive Chairman of Moven

Brett King

@BrettKing

King is a futurist, a bestselling author, an award winning speaker, and banking revolution advocate. He created the popular radio show Breaking Banks in 2013. After the show gained international acclaim, King launched smart banking app Moven, which has received almost $50 million US in venture funding. King's primarily interest is how modern technologies are disrupting business, changing behaviour, and influencing society.

Co-founder & CEO of Chain

Adam Ludwin

@adamludwin

Ludwin rose to fame in 2016 when his startup Chain secured deals with Visa and other major financial institutions, bringing 'true' Blockchain to an important area of the mainstream economy. Chain continues to expand, while Ludwin has become a vocal online presence on Blockchain and cryptocurrency.

Founder & CEO of ConsenSys

Joseph Lubin

@ethereumJoseph

Lubin is a worldwide famous distributed database entrepreneur. Before co-founding Ethereum, he worked as research staff in the Robotics Lab at Princeton, as well as at Vision Applications, Inc and various posts in field of technology.

Co-founder of Coinbase

Fred Ehrsam

@FEhrsam

A former Wall Street trader and writer at the Duke Journal of Economics, Ehrsam shifted his interests into the crypto industry in 2012 when he co-founded Coinbase, an online payment system with the stated mission of making Bitcoin easy to use. Ehrsam has been named in TIME Magazine's 30 Under 30 Who Are Changing the World (2013) and listed as one of Forbes 30 Under 30 (2014).

Co-founder of Ztudium

Dinis Guarda

@dinisguarda

Guarda is globally-recognized top influencer, digital and crypto economics driver, evangelist and leader in fintech and Blockchain industries. With over 20 years experience in international business and digital transformation, Dinis has worked with new tech, cryptocurrencies, drive ICOs, regulation, compliance, legal international processes, and has created and been involved in various top 100 digital currencies. He is ranked as one of the most influential people in Blockchain in the world by Right Relevance.

Founder & CEO of Galaxy Digital

Michael E. Novogratz

@novogratz

Novogratz was formerly a member of the board of directors of Fortress Investment Group LLC and Chief Investment Officer of the Fortress Macro Fund. Novogratz joined Fortress in 2002 after spending 11 years at Goldman Sachs, where he was elected partner in 1998. Novogratz has founded and serves as the Chairman of the Board for Beat the Streets, a non-profit organization which builds wrestling programs in New York City public schools, and is also the Honorary Chairman of USA Wrestling Foundation.

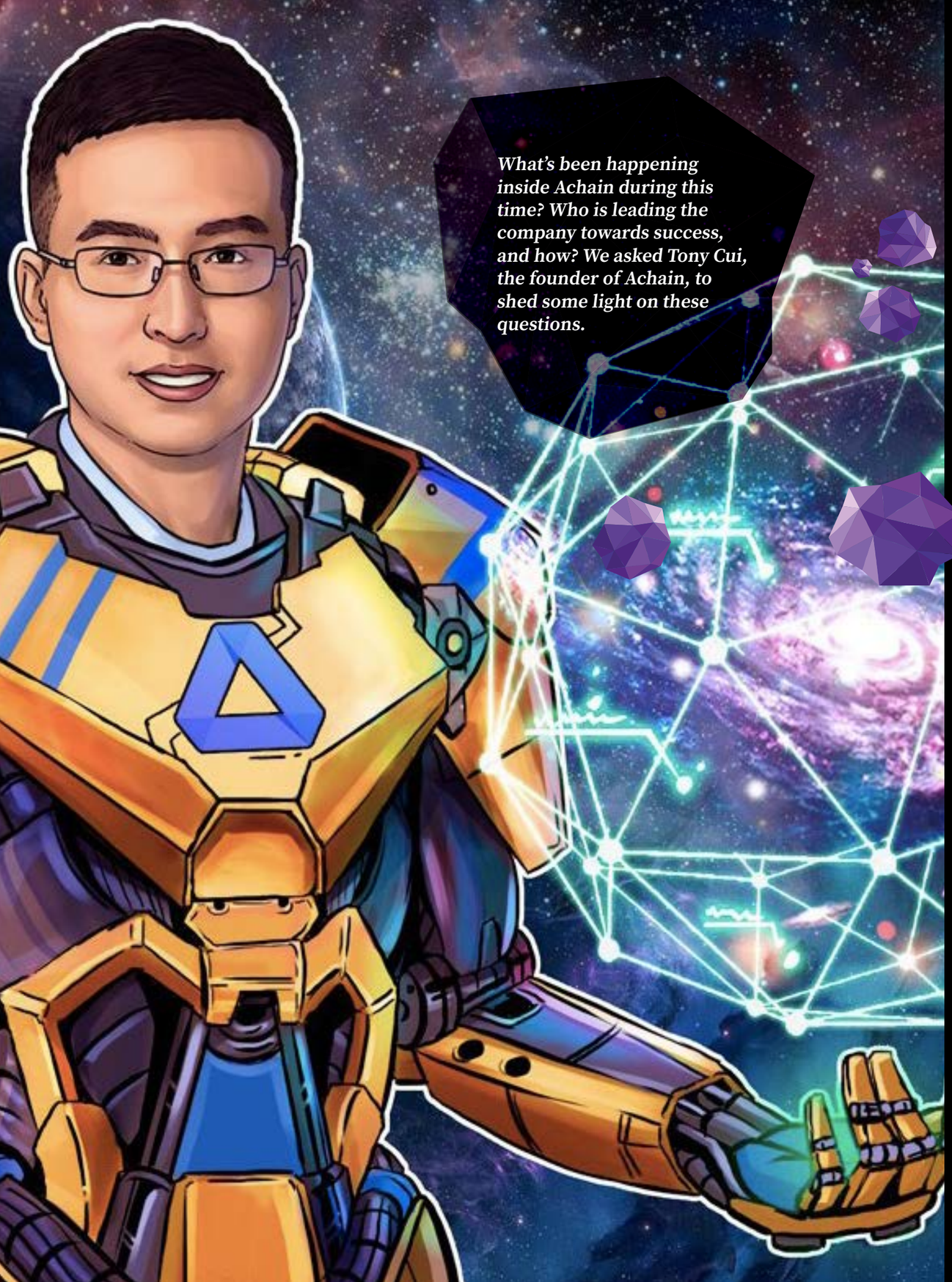
Owner, Editor & Publisher
of the Digital Banking Report

Jim Marous

@JimMarous

Marous is an internationally recognized financial industry strategist. He is named one of the most influential people in banking and a Top 5 Fintech Influencer. Apart from his writing and publishing, he advises on customer experience, portfolio growth, innovation, marketing strategies, channel shift and digital transformation within the financial services industry.

More people on
top.cointelegraph.com



Achain

DREAMING, BELIEVING, LIVING

THE STORY OF ACHAIN THROUGH THE FOUNDER'S EYES

The first time we met Achain was last November at BlockShow Asia 2017. Back then, the company's representatives were opening the conference with a welcoming speech. This year, the company is coming back to join BlockShow Europe 2018 in Berlin.

SO WHAT IS ACHAIN?

First let's get some context. Achain is a public Blockchain platform that enables developers of any level to issue tokens and create smart contracts, decentralized applications, and Blockchain systems. The main purpose of this platform is to build a global Blockchain network for information exchange and value transactions.

> *"In the company, the boss says, and the employees do, regardless of if they agree. When two people are consistent on the surface and inconsistent in heart, the results will never satisfy. However, in a community, people are more willing to express themselves fully and participate actively."*

MUSTN'T BE AFRAID TO DREAM A LITTLE BIGGER, DARLING

Cui Meng's life changed forever in 2012, when his friends introduced him to Bitcoin; since then, he completely devoted his energy into building something that he and his team passionately believe in. But the path to success required plenty of sacrifices and risks as he navigated very much unchartered territory. The story of Achain resonates across the Blockchain community as one of success, perseverance, and determination despite the numerous challenges along the way.

DREAMING IS BELIEVING

Most crypto projects aim for the moon; Achain, however, has always dreamt bigger, and with the completion of the first development phase, the team is now ready to take on the next phase, the so-called "Galaxy Phase". The transition from Singularity to Galaxy will allow the team to build a connected Blockchain system that will empower the users, regardless of whether it's enterprise solutions or individuals. 2018 is set to be a positive and crucial year for Achain.

SHARING IS CARING

In Tony Cui's eyes, Achain's tens of thousands of token holders are the same as Achain's full-time team: they are all members of the community. In the community, the motto is that "we are equal regardless of our ability to influence".

> "The subset of the community is the company. We only make rules and incentive for thecommunity. How much profit you make is dependent on how much effort you put in."

The above is very much in the spirit of Blockchain and an environment of trust, something that traditional systems do not cater to. As a result of this emphasis on sharing, as well as global reach expansion, Achain has been very proactive in quietly growing its bases and social community channels in Singapore, South Korea, and the US. Being at the heart of the ICO world has its benefits, but there are also plenty of drawbacks.

DO YOUR ACTIONS MATCH YOUR WORDS?

Achain is looking for solutions that provide developers with ready-to-use Blockchains from the start. Cross-chain communication is one of the challenges and it is an essential part of building a boundless Blockchain world. Breaking down this barrier will bring more utility; this makes Blockchains powerful.

To summarize, Tony Cui states:

"The year 2018 is a turning point for Achain. Now we are transitioning from phase one Singularity to phase two Galaxy, where we will build a connected Blockchain system that will empower corporations and individuals alike. We feel deeply grateful and fortunate to have such a strong and amazing community who made so many contributions to Achain. With you, the Achain ship will surely sail among the stars."

FUN

LIFE TOKENIZED:

THE BLOCKCHAIN REALITY SHOW EXPERIENCE

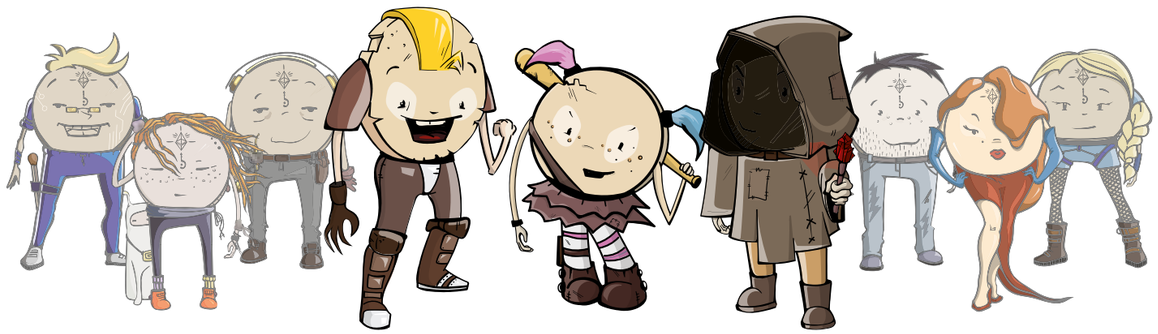
The final episode of Deus ETH, the first survival show on Blockchain that combines elements of a reality show with a lottery and a visual novel, was broadcasted on April 13, 2018.

HOW DEUS ETH WORKS?

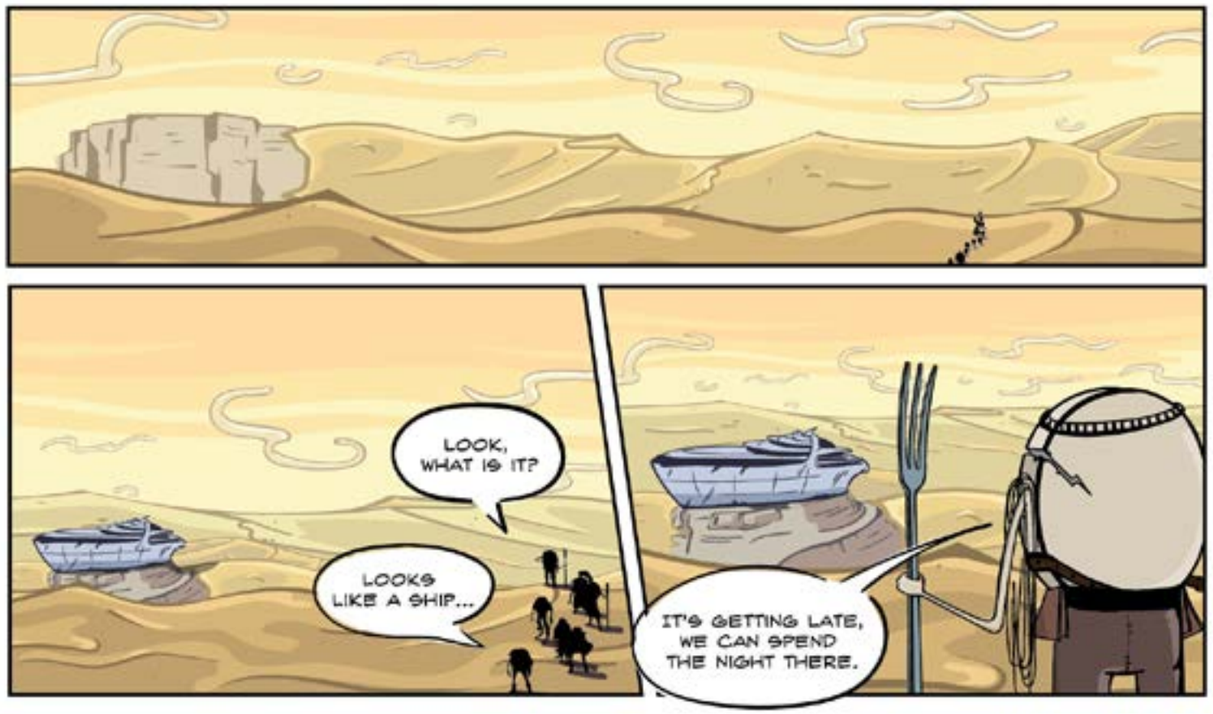
Over the course of 10 episodes, 50 tokens went through a sequence of events simulated by smart contracts. All the heroes had an equal chance of survival, and only the smart contract could decide who was to die and who was safe for another episode. The novel's ending was unknown to everyone until the very end of the show.

THE WINNERS

The viewers of Deus ETH bought characters for Ethereum and followed the storyline. The owners of the three characters who reached the end of the show shared a prize of 13,59 ETH (~$6800).



The second episode of the show was enacted in a comic strip format. It describes the adventures of the wounded tokens who continue their search for the promised land. Suddenly, they come across a luxurious but shabby yacht stuck in the sand. Surprisingly, it is inhabited by hospitable wolves, who kindly invite the tokens to refresh themselves and spend the night. Most of the tokens believe that this is a trap, and continue on their journey. However, some of them accept the wolves' invitation.


LOOK, WHAT IS IT?
LOOKS LIKE A SHIP...
IT'S GETTING LATE, WE CAN SPEND THE NIGHT THERE.

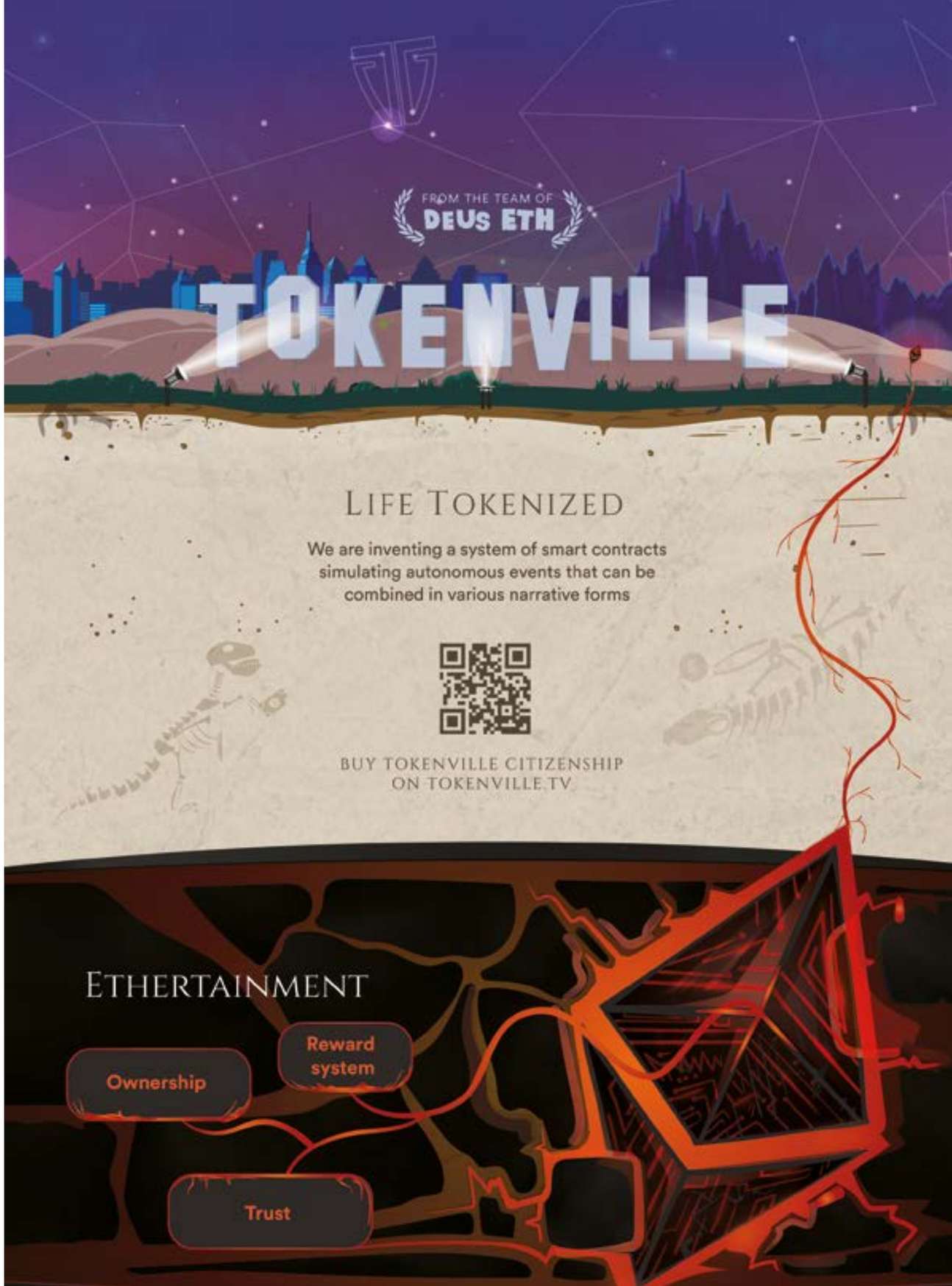

HOW MANY OF THEM?
ENOUGH FOR ALL OF US. PULL THE SWITCH.
SWOOSH
Order: Carnivora
Family: Traders
Genus: Canis
Species: Stylish
Hair pomade Philip ETH
(pure gold from roots to tips)
Money ETH
(the anthem of success)
Shirt Kethton
(for rich wolves only)
Tie Charveth
(too pricey for you)
Suit Brethoni
(tailored on demand)
Shoes ETH Ford
(to die for)
DEUS ETH


I DEFINITELY LIKE IT HERE, SIR
BROTHER, RESIST THE EVIL TEMPTATION!
YOUR MORALS MAKE NO SENSE!
GET OUT AND GOOD LUCK TRYING TO FIND YOUR PROMISED LAND
WELCOME, DEAR TRAVELERS
YOU CAN REST AND REFRESH YOURSELF HERE AT OUR PLACE
AND JUST FOR YOU TO KNOW, IT'S ABSOLUTELY FREE OF CHARGE
WE ARE STAYING!


WOW
!
WHERE DO WE START FROM?
I CAN'T BELIEVE MY OWN EYES!
WHAT WOULD YOU LIKE, MADAM?
WE HAVE SOME FINEST LONG-TERM INFLATION, AN EXCELLENT COCKTAIL OF SPECULATION AND DEFICIT
HMM
HMM

CHECK THEM OUT!

Other episodes, as well as the names of the winners, are available on the website:



PROOF-OF-WORK EXPLAINED

1. What is Proof-of-Work?
2. What do you mean a “mathematical puzzle?”
3. How come?
4. How is this algorithm implemented in Blockchain?
5. And where PoW is usually implemented?
6. Which trends should we expect in the future?
7. Any flaws in the PoW consensus algorithm?
8. 51% attack, what are you talking about?

What is Proof-of-Work? 1

Proof-of-Work, or PoW, is the original consensus algorithm in a blockchain network.

In blockchain, this algorithm is used to confirm transactions and produce new blocks to the chain. With PoW, miners compete against each other to complete transactions on the network and get rewarded.

In a blockchain network, users send each other digital tokens. A decentralized ledger gathers all the transactions into blocks. However, care should be taken to confirm the transactions and arrange blocks.

This responsibility bears on special nodes called miners, and a process is called mining.

The main working principles are a complicated mathematical puzzle and a possibility to easily prove the solution.

What do you mean a “mathematical puzzle?” 2

It’s an issue that requires a lot of computational power to solve.

There are a lot of them, for instance:

- a*hash function,* or how to find the input knowing the output.
- *integer factorization. In other words, how to present a number as a multiplication of two other numbers.*
- *guided tour puzzle protocol. If the server suspects a denial of service (DoS) attack, it requires a calculation of hash functions, for some nodes in a defined order. In this case, it’s a ‘how to find a chain of hash function values’ problem.*

The answer to the PoW problem or mathematical equation is called a hash.

As a network grows, it faces more and more difficulties. The algorithms need more and more hash power to solve. So, the complexity of the task is a sensitive issue.

How come? 3

Accurate work and the speed of the Blockchain system depend on it.

However, the problem shouldn’t be too complicated. If it is, the block generation takes a lot of time. The transactions are stuck without execution and as a result, the workflow hangs for some time. If the problem cannot be solved in a definite time frame, block generation will be kind of a miracle.

On the flip side, if the problem is too easy it is prone to vulnerabilities, DoS attacks and spam.

The solution needs to be easily checked. Otherwise, not all nodes are capable of analyzing if the calculations are correct.

Then you will have to trust other nodes and it violates one of the most important features of blockchain – transparency.

How is this algorithm implemented in Blockchain? 4

Miners solve the puzzle, form the new block and confirm the transactions.

How complex a puzzle is dependent on the number of users, the current power and the network load. The hash of each block contains the hash of the previous block, which increases security and prevents any block violation.

If a miner manages to solve the puzzle, the new block is formed. The transactions are placed in this block and considered confirmed.

Where is PoW usually implemented? 5

Proof-of-Work is used in a lot of cryptocurrencies.

The most famous application of PoW is Bitcoin. It was Bitcoin that laid the foundation for this type of consensus. The puzzle is Hashcash – this algorithm allows changing the complexity of a puzzle based on the total power of the network. The average time of block formation is 10 minutes. Bitcoin-based cryptocurrencies, such as Litecoin, have a similar system.

Another large project with PoW is Ethereum. Given that almost three of four projects are implemented on the Ethereum platform, it’s safe to say that the majority of blockchain applications use PoW consensus model.

Why use a PoW consensus algorithm in the first place? 6

The main benefits are the anti-DoS attacks defense and low impact of stake on mining possibilities.

Defense from DoS attacks. PoW imposes some limits on actions in the network. They need a lot of effort to be executed. Efficient attacks require a lot of computational power and a lot of time to perform the calculations. Therefore, the attack is possible but kind of useless since the costs of carrying out the attack are too high.

Mining possibilities. It doesn’t matter how much money you have in your wallet. What matters is to have large computational power to solve the puzzles and form new blocks. Therefore the holders of huge amounts of money are not in charge of making decisions for the entire network.

EXPLAINED

Any flaws in the PoW consensus algorithm? 7

The main disadvantages are huge expenditures, "uselessness" of computations and 51 percent attacks.

Huge expenditures. Mining requires highly specialized computer hardware in order to run the complicated algorithms. The costs are unmanageable – as a result, mining is becoming available only for special mining pools. These specialized machines consume large amounts of power to run that increase costs. Large costs threaten centralization of the system since it benefits only those who can afford it. It is easy to see in the case of Bitcoin.

Uselessness of computations. Miners do a lot of work to generate blocks and consume a lot of power. However, their calculations are not applicable anywhere else. They guarantee the security of the network but cannot be applied to business, science or any other field.

51 percent attack – what does this mean? 8

A 51 percent attack, or majority attack, is when a user or a group of users control the majority of mining power.

They can monopolize generating new blocks and receive rewards since they're able to prevent other miners from completing blocks. They can reverse transactions.

As an example, let's assume Alice sent Bob some money using blockchain. Alice is involved in the 51 percent attack case, Bob is not. This transaction is placed in the block. But the attackers don't let the money be transferred. There is a fork happening in the chain.

Further, miners join one of the branches. As they have the majority of the computational power, their chain contains more blocks.

In the network, a branch that lasts longer remains, and shorter one is rejected. So, the transaction between Alice and Bob does not take place. Bob doesn't receive the money.

Following these steps, the attackers can reverse transactions.

A 51 percent attack is not a profitable option. It requires an enormous amount of mining power. Once it gets public exposure, the network is considered compromised, which leads to the outflow of users. This will inevitably move the cryptocurrency price down. As a result, the funds lose their value.

ESCROW EXPLAINED

1. What is an escrow?
2. How does it work?
3. What is a threshold scheme?
4. Is it secure?
5. If escrow is that good, why does not everybody use it?
6. How is escrow applied in the Blockchain world?

What is an escrow? 1

An escrow is a way to control and protect financial assets.

An escrow is a legal concept where a financial instrument or an asset is held by a third party on behalf of two other parties that are in the process of completing a transaction. In other words, when you use an escrow, a third-party acts as a guarantor. The funds or assets are held by the third-party, also known as an escrow agent. The escrow agent controls the whole process and makes sure the commitments are fulfilled. Therefore, nobody can use money on their own without the agreement from other participants.

How does it work? 2

One of the most used concepts is a secret splitting.

Escrows work when you possess important information and share it with people and/or companies you trust. You can share a password, a number of a bank account, an access to securities, and more. No one can get access on their own. The only way to access it is with a mutual agreement.

However, there are some weak spots. If one party loses access to the info and has no connection with other parties to make an agreement or compromises themselves and loses trust, there is no way to restore it.

What if you can't gather or reach all the people involved? Consider a threshold scheme.

What is a threshold scheme? 3

A threshold scheme is an improved version of secret splitting.

The threshold scheme does not require the agreement of all parties. For example, you share info with five different parties, but any three of them can reconstruct the secret. Two parties are not enough to get access to the info. If you need to exclude someone from your escrow, you can do it without any difficulties. These parties can be divided into groups, depending on the confidence level. Let's assume you have six people, you completely trust three of them – group one, and the other three are less credible – group two.

You can make a scheme of data reconstruction, in case something happens. So the access is available to three people from group one and anyone from group two. Or any two people from group one and three people from group two. There are no restrictions in the threshold system. They can be as complex and easy as you wish.

Is it secure? 4

Mathematics and cryptography prove the reliability of the escrow.

A lot of mathematicians and cryptologists have worked on the security issue and managed to develop algorithms for safe escrow. A lot of research was made to improve the security of escrows. To avoid collusion of parties, a scheme was developed where some are able to cancel the decision of others. If a party tries to cheat, there is a way to thwart their plans. If some party loses their access, there is no need to change the key.

If escrow is that good, why doesn't everybody use it? 5

Complexity of implementation discourages a lot of people.

The described models are rather complicated. It's much more difficult to understand it than it might look. You'll most likely need an individual expert in mathematics and cryptography in the team. Moreover, incorrect implementation can be costly. You may not notice any mistake in the system at first, but it may make it vulnerable or the funds unavailable.

Don't forget about guarantors. They put their reputation at stake. Certainly, their services will cost a lot. Together with the expert, expenses will significantly increase.

How is escrow applied in the Blockchain world? 6

Escrow is gaining more and more popularity in blockchain.

A lot of companies understand the importance of guarantees for investors to prevent scams. The team may be unknown to the general public, but the Blockchain world has its authorities which reputation is indisputable. Some companies serve as a third party in different agreements. Some startups already launch their ICOs with escrow. The largest blockchain platform, Ethereum, has already made an escrow smart contract. Escrow can become one of the power instruments to show the seriousness of your project.

BITCOINS FUTURES EXPLAINED

1. What are futures?
2. How do futures contracts work?
3. What are Bitcoin futures?
4. How do they work?
5. What do Bitcoin futures mean for the Bitcoin price?
6. Does it mean the price is most likely to go up?
7. What do they mean for the whole blockchain industry?
8. Where can you trade Bitcoin futures?

What are futures? 1

Futures are an agreement to buy or sell an asset on a specific future date at a specific price.

Once the futures contract has been entered, both parties have to buy and sell at the agreed upon price, irrespective of what the actual market price is at the contract execution date.

The goal is not necessarily profit maximization. Futures are a risk management tool, often used in financial markets to hedge against the risk of changing prices of assets that are bought and sold on a regular basis.

Futures are also used in portfolios to balance out price fluctuations on investments, where the underlying asset is particularly volatile.

These contracts are negotiated and traded on a futures exchange which acts as the intermediary.

How do futures contracts work? 2

There are two positions you can take on a futures contract: long or short.

If you take a long position, you agree to buy an asset in the future at a specific price when the contract expires. When you take a short position, you agree to sell an asset at a set price when the contract expires.

A good way to explain this is using the example of an airline who wants to hedge against the rising price of fuel by entering into a futures contract.

> *Say jet fuel trades at $2 per gallon. An airline expecting the price of oil to rise, buys a three-month futures contract for 1,000 gallons at current prices. The contract is, therefore, worth $2,000.*
>
> *If in three months, when the contract expires, the price of one gallon of jet fuels is $3, the airline saved $1,000.*

The supplier will happily enter into a futures contract in order to ensure a steady market for fuel, even when prices are high. And the same contract will also protect them if the price of fuel unexpectedly drops.

In this case, both parties are protecting themselves against the volatility of fuel prices.

There are also investors who speculate with futures contracts rather than using it as a protection mechanism.

They will deliberately go long when the price of a commodity is low. As prices rise, the contract becomes more valuable, and the investor could decide to trade the contract with another investor before it expires, at a higher price.

What are Bitcoin futures? 3

Futures are not just for physical assets; they can be traded on financial assets as well.

With Bitcoin futures, the contract will be based on the price of Bitcoin and speculators can place a “bet” on what they believe the price of Bitcoin will be in the future.

In addition, it enables investors to speculate on the price of Bitcoin without actually having to own Bitcoin.

It has two major consequences.

First, while Bitcoin itself remains unregulated, Bitcoin futures can be traded on regulated exchanges. This is good news for those who are concerned about the risks related to the industry’s lack of regulation.

Second, in areas where trading Bitcoin is banned, Bitcoin futures allow investors to still speculate on the price.

How do they work? 4

A Bitcoin future will work on exactly the same principles as futures on traditional financial assets.

By anticipating whether the price of Bitcoin will go up or down, speculators will either go long or short on a Bitcoin futures contract.

> For example, if an individual owns one Bitcoin priced at $18,000 (hypothetically) and foresees that the price will drop in the future, to protect themselves, they can sell a futures contract at the current price, which is $18,000.
>
> Close to the settlement date the price of Bitcoin, along with the price of the Bitcoin futures contract, would have dropped. The investor now decides to buy back the Bitcoin futures.
>
> If the contract trades for $16,000 close to the future settlement date, the investor has made $2,000 and therefore protected their investment by selling high and buying low.

This is a basic example of how Bitcoin futures work and the exact terms of each future contract may be more complex depending on the exchange, which will include minimum and maximum price limits.

What do Bitcoin futures mean for Bitcoin's price? 5

In the short-term, it pushes the price upwards as the overall interest in the cryptocurrency spikes.

The day after Bitcoin futures were launched on the Chicago Board Options Exchange (CBOE), for the first time on a major regulated exchange, the price jumped by almost 10 percent to $16,936.

Similarly, in the run-up to the launch of Bitcoin futures on one of the world's biggest exchanges the Chicago Mercantile Exchange (CME), Bitcoin's price broke through the $20,000 barrier.

Does it mean the price is most likely to go up? 6

There are several reasons why this is the case.

- As Bitcoin futures can be regulated on public exchanges, it gives people who were previously skeptical as a result of the lack of regulation the confidence to invest.
- Institutional investors are more likely to offer Bitcoin futures to their clients as a viable investment option.
- It brings more liquidity to the market, making it easier to buy, sell and trade the cryptocurrency, and therefore much more lucrative.
- It opens up the Bitcoin market to a wider investor base, including countries where the trade of Bitcoin has been banned.

As futures are designed to balance out price fluctuations of underlying assets, it could also make the price of Bitcoin less volatile.

What do futures mean for the whole Blockchain industry? 7

There are various possible outcomes.

First, Bitcoin is seen as a sort of poster-boy for cryptocurrencies. Therefore, if the price of Bitcoin sees massive increases in a short space of time, irrespective if this is due to Bitcoin futures or otherwise, more people tend to take notice.

As more people become aware of the cryptocurrency industry, the uptake of altcoins will increase and push prices upwards.

The flipside is also possible; investors might want to sell their altcoins for Bitcoins in order to take part in its bullish run. Large-scale exits could cause a drastic drop in the price of alternative cryptocurrencies.

The more likely scenario is that some of the stronger altcoins, like Ethereum, Litecoin, Ripple, etc., might follow in the footsteps of Bitcoin and become tradeable as futures as well, once interest from investors become strong enough.

Where can you trade Bitcoin futures? 8

There are two separate markets where Bitcoin futures can be traded.

The second option is on publicly regulated exchanges. This is a recent phenomenon and part of the reason why we've seen the Bitcoin price hike during December 2017.

It started with CBOE's Bitcoin futures launch on the Dec. 10. The CME followed with its launch on Dec. 17 and trading on Dec. 18. Brokerage firms like TD Ameritrade and JP Morgan have also expressed their interest to allow access to these markets.

ANALYSING ICO EXPLAINED

1. Why compare ICO's?
2. How can I do it?
3. I've also heard about the MVP, what's that?
4. Should I pay attention to the social media?
5. Should I listen to experts' opinion?
6. Is it possible to automate the project's evaluation?

Why compare ICO's?

1

Comparing ICO's can be beneficial to both cryptocurrency investors as well as the ICO teams themselves.

Different parties will have different reasons for wanting to know how an ICO compares to the rest of the market.

For investors, it would be to establish if a particular product has the potential of delivering the expected return on investment in the long-run and which option would be the best to commit to when looking at similar projects.

For ICO teams themselves, it can be beneficial to look at other token sales that rate particularly well to determine which area of their project they need to work on or improve in order to achieve a similar level of success.

Then there's the general enthusiast who's interested to see what the rest of the market thinks about a particular ICO and to what extent the solution provided has the potential to be truly revolutionary.

The problem is there are multiple ICO's launched daily which equates to thousands every year. Some of the projects will be similar and there are bound to be a few not so great products in between.

With so many token sales flooding the market, it can be overwhelming and difficult to separate the good ones from the bad ones without having to do an in-depth and time-consuming analysis on individual ICO's and their target market.

How can I do it?

2

The most effective way is to create a rating system based on a number of crucial ICO success indicators.

This will include the team behind the project, information on the ICO itself, how the product is presented and how well it is marketed.

The team: It is important for profiles on team members to be easily accessible and a sufficient amount of information should be disclosed on each individual. Displaying photos and links to external professional sites such as LinkedIn will help to instil trust and credibility.

Furthermore, the number of team members involved can also be a decisive rating factor. If there are only two individuals working on the project, you know it's unlikely to be successful. However, multiple people are working on different aspects of the ICO, the chances of success are much bigger.

ICO information: Information on the actual ICO should be clearly visible and available. Start and end dates on pre-sales and the official ICO, how individuals can buy into the crowd sale and what currencies are accepted, a countdown towards the start and end of the sale, and the price of each token can all help to take out the guesswork for investors which will give them more confidence to commit.

How the product is presented: This will depend largely on the information available in the whitepaper. It should include what the product is – for example, the platform, service, etc., different milestones the company hopes to achieve and when they plan to achieve them, more detailed information on team members and the actual uses of the digital token. Having a professional video presentation with an overview of the product shows further quality and commitment from the ICO team.

I've also heard about the MVP, what's that?

3

MVP, or Minimum Viable Product, is a product with a minimum set of features enough to satisfy customers' needs.

Generally, it is a prototype, alpha or beta version of the future product. It is used to get feedback and make changes in the project. It's not yet a common thing in the crypto industry, but if it's available, it definitely increases investors' trust in the product.

An open code allows to see if the company has any groundwork. You can check the implementation of the concept described in whitepaper and the progress of work on the product: optimization, fixing bugs, functional extension, etc.

A non-programmer might not fully grasp the code but they can rely on the opinion of people in good standing.

Should I pay attention to social media?

4

You definitely should!

With so many ICO's being launched on to the market, it is essential for individual projects to attract a sufficient amount of attention to their product. The best way to judge this is by the marketing efforts of the company.

Are they active on different social media sites like Facebook, Twitter or Medium? Do they have a presence in relevant cryptocurrency forums like BitcoinTalk and GitHub? And what sort of information are they putting out there? These are all important questions to answer when comparing ICO's.

5 Should I listen to experts' opinion?

One of the most important factors to look at when rating ICO's is the opinions of the experts in the cryptocurrency world.

They would broadly look at the same criteria but from a different angle.

Team: Teams with relevant cryptocurrency experience are generally rated much stronger than complete industry novices.

This includes experience in development, coding, project management, community management and marketing. The presence of an advisory board will further improve the integrity of a particular project.

Product information: ICO's generally have two different aims. One is the funding of a completely new concept; the other is to fund the expansion of an existing project or to move it onto a blockchain-based network. The latter is more likely to see success as it's based on an already proven product or service. Therefore, experts will favor these projects.

A product or service that addresses an actual problem in the market can also enjoy a higher rating.

Business know-how: Projects with clearly defined long-term goals, a stated plan on how to achieve it, and the amount of investment needed to get there will be more likely to see success. Experts will also pay attention to whether or not there's an already existing user base and if a competitive analysis has been done to better understand the playing field.

Market robustness: The ICO industry is mostly unregulated. This can change at any minute and different legislature can be implemented in different regions. A project with the flexibility to adapt and overcome changing market conditions should receive a higher comparative rating.

6 Is it possible to automate the project's evaluation?

It is and it'll definitely speed up the process.

Cooperation of human and artificial intelligence (AI) can facilitate the assessment.

AI has taken significant steps forward in recent years, and its capacities have increased considerably. Nevertheless, it still should have some basis to work properly. People's opinions about different project may be used as a base. The program will analyze the behavior of the participant according to set parameters and be able to make its own decision about the projects. Further, the network and people work together. Next users' assessments will maintain the database of the program and improve its works. The network will grade the projects and help undecided people.

This process flow has been realized in practice by a project called DropDeck. The projects will be ranked by using AI for investors.

**Disclaimer. Cointelegraph does not endorse any content or product on this page. While we aim at providing you all important information that we could obtain, readers should do their own research before taking any actions related to the company and carry full responsibility for their decisions, nor this article can be considered as an investment advice.*

BLOCKSHOW EUROPE 2018

YEARBOOK

Addy Crezee
CEO

Anna Sergius
Deputy Director

Vlad Stoiny
Sponsor Relations

Katrin Demi
Sponsor Relations

Daria Kort
Event Manager

Elaine Mcqueen
Assistant Manager

Alex Kotezky
Designer

Julia Daimio
Agenda&Research Expert

Victoria Neiman
Project Manager

Aleksander Raserei
Artists&Content Manager

Lina Freeman
Public Relations Manager

Stefania Rossi
Media Relations

Shavrat Gas
Partner Relations

Aleksandra Miller
Account Manager

Florence
Ibuowo Olubunmi
Call Center Operator

John Fom
Media Buyer

Stasy Dulcimer
Media Producer

Roma Markiz
Videomaker

Nadia Odom
Creative Producer

Ksenia Eris
Customer Support

Daria Blumgart
Email Marketing Expert

Andrew Helga
Product Manager

Tanya Krum
Social Media Manager

Tony Hudson
Marketing Expert

Xenia Radomski
Event Manager
for Americas Region

Executive editor: Stacy Dunay. Chief designer: Valentine Alise

Authors: Kajsa Söderlund, Stacy Dunay, Andrew Tar, Markus Kasanmascheff, Kirill Bryanov, Chrisjan Pauw, Stephen O'Neal, Nikolai Kuznetsov, Veronika Rinecker

Cointelegraph Special Edition was published under Cointelegraph franchise. Learn more: **cointelegraph.com/franchise**

BLOCK SHOW

POWERED BY

COINTELEGRAPH

The Future of Money

Cointelegraph
BlockShow Edition
May 14, 2018
Not for Sale