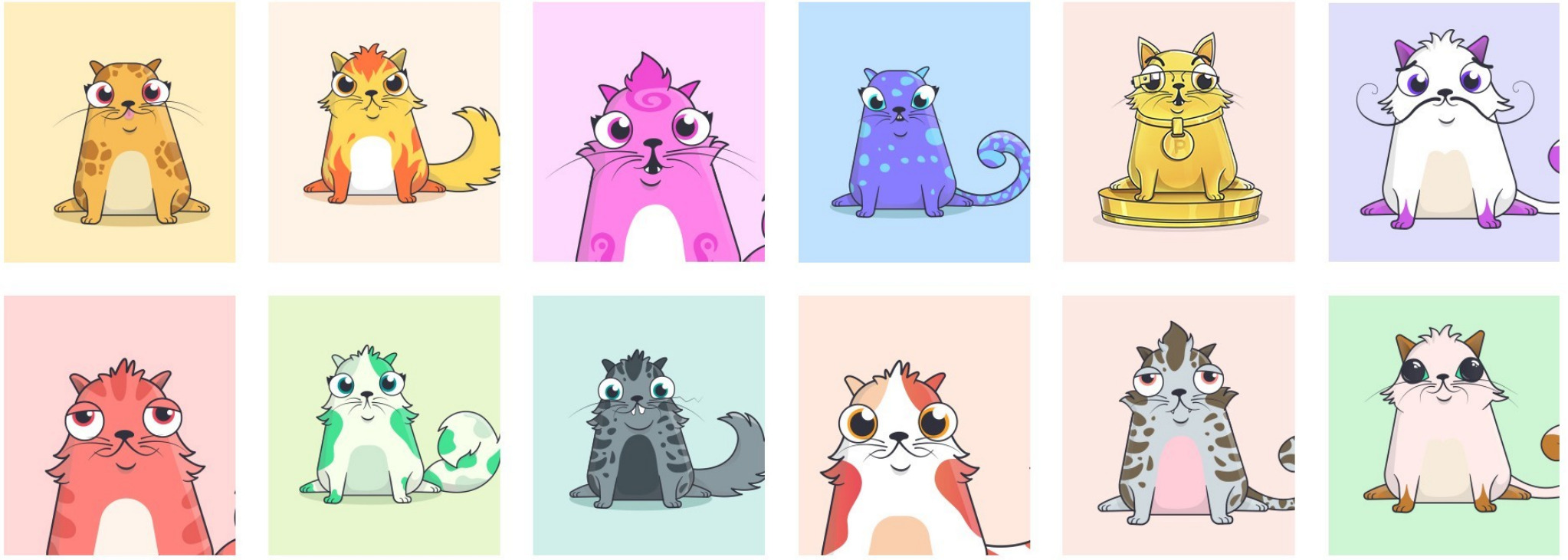
NFT. Top 2021 blockchain trend

CryptoKetties 2017

NBA Top Shots marketplace 2018



ERC721 NFT

```
    function balanceOf(address _owner) external view returns (uint256);
    function ownerOf(uint256 _tokenId) external view returns (address);
    function safeTransferFrom(address _from, address _to, uint256 _tokenId,
bytes data) external payable;
    function safeTransferFrom(address _from, address _to, uint256 _tokenId)
external payable;
    function transferFrom(address _from, address _to, uint256 _tokenId)
external payable;
    function approve(address _approved, uint256 _tokenId) external payable;
    function setApprovalForAll(address _operator, bool _approved) external;
    function getApproved(uint256 _tokenId) external view returns (address);
    function isApprovedForAll(address _owner, address _operator) external
view returns (bool);
```

ERC1155 NFT MultiTokens

```
// ERC-20
function transferFrom(address from, address to, uint256 value) external
returns (bool);

// ERC-1155
function safeBatchTransferFrom(
    address _from,
    address _to,
    uint256[] calldata _ids,
    uint256[] calldata _values,
    bytes calldata _data
) external;
```

Ecommerce and Blockchain Services and Exchange

Stripe (JS integrated API, modern, high security, 2.9% +30 cents fee)

2Checkout (200 countries, 3.5-6% fees)

Fondy.eu (better card processing, 1.2-1.8% fee)

BitPay (accept BTC, withdraw in fiat currency, 1% fee)

Binance (largest crypto exchange)

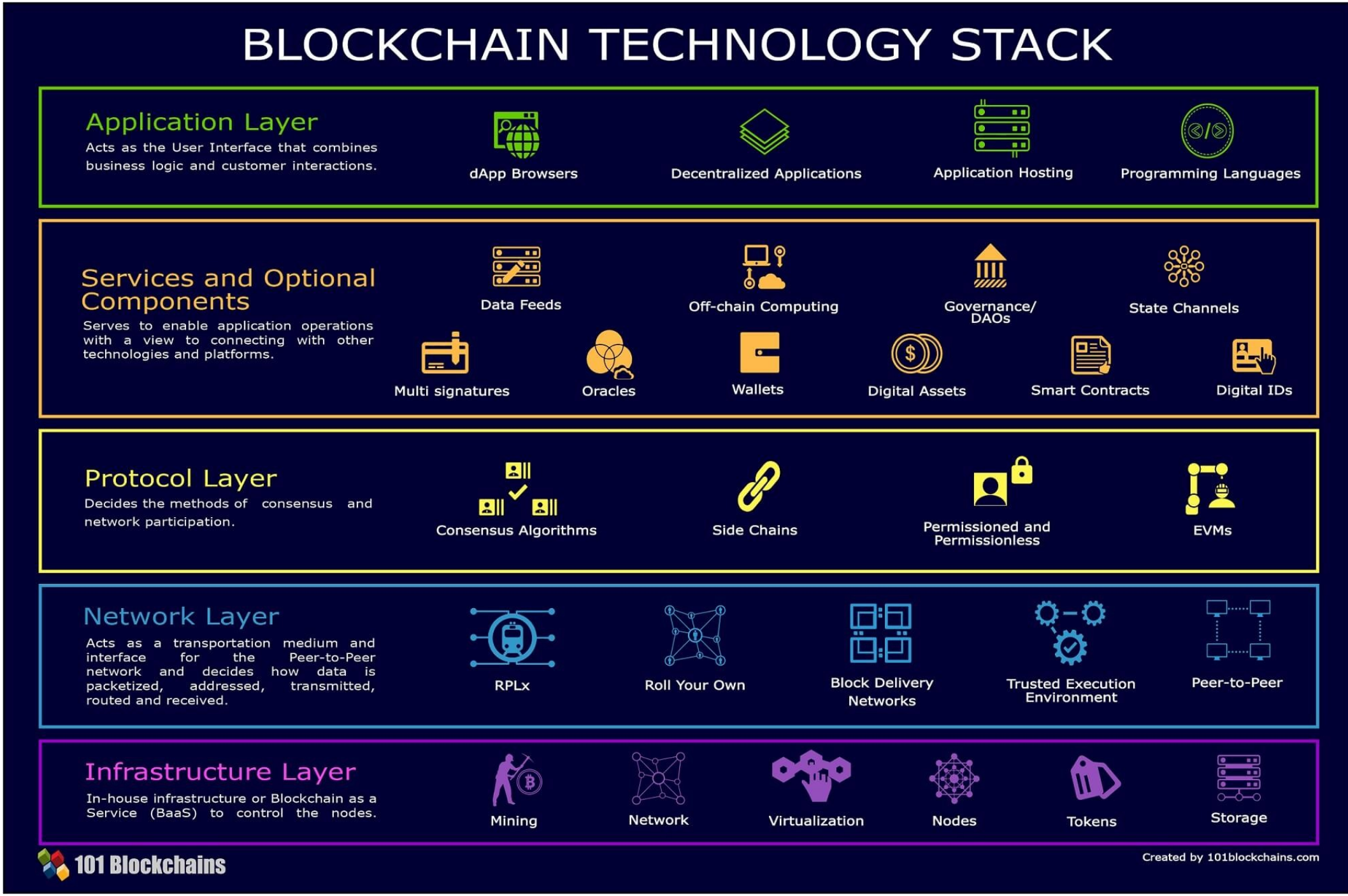
CoinBase.com (popular exchange + API, accept cryptocurrecy)

CoinAPI.io (realtime cryptocurrency exchange rates API from 300+ exchanges, historical data)

coinmarketcap.com (enterprise-grade cryptocurrency API, exchange rates, historical data)

OpenSea.io (NFT marketplace)

Web 3.0 Technology Stack



Source: https://101blockchains.com/web-3-0-blockchain-technology-stack

Decentralized Atonomous Organization (DAO)

Has refined rules and goals.

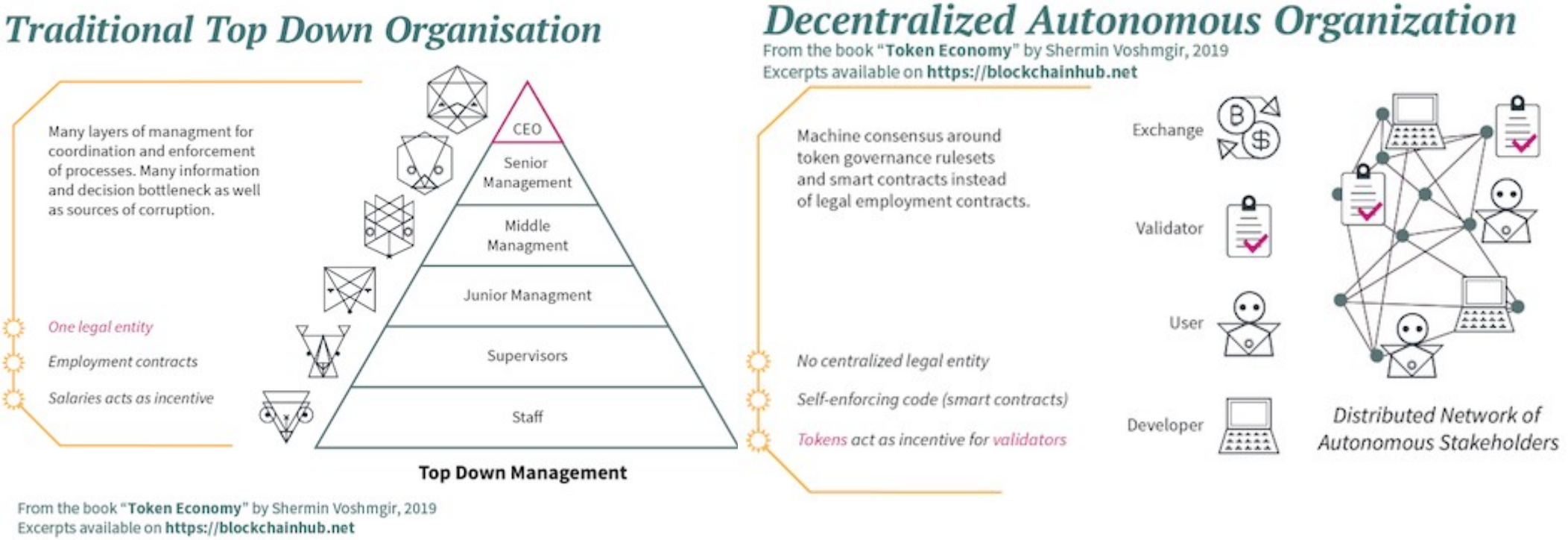
Operated by smart contract.

Distributes votes to members during funding phase.

Deployed to public blockchain, usualy via special web service:

Aragon.org, Daostack.io

Epic FAIL:
The DAO launched with $150 million in crowdfunding in June 2016,
was hacked and drained of US$50 million in cryptocurrency.
Cused Ethereum to fork on
Ethereum Classic (ETC) and Ethereum (ETH).



101 Blockchains | DIGITAL IDENTITY: A SIMPLE EXPLANATION

WHAT IS DIGITAL IDENTITY?

A digital identity is a type of identity format where an individual's identity is represented through digital means.

WHAT IS SELF-SOVEREIGN IDENTITY (SSI)?

A self-sovereign Identity is actually a form of digital identity that solely belongs to the individual or organization. It means that the owner will have full control over the data and sharing ability.

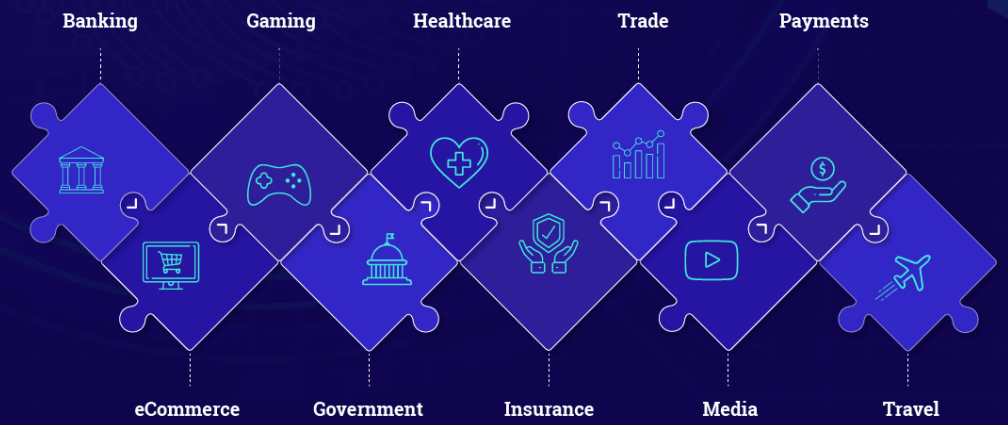
ISSUE OF TYPICAL IDENTITY MANAGEMENT SYSTEM

- Bad Password Combination
- Failure due to Manual Provisioning and De-Provisioning Process
- No regulations for access restriction
- Low Security for identities in devices and browser
- Applications not being up to date
- Not utilizing security measures
- Multiple administrative models for multiple application creates inconsistency
- Lack of device management with an identity In BYOD
- Same Repetitive KYC or registration process
- Identity risk
- Weak Authentication Protocols
- Only Centralized servers giving out identities
- Companies can easily mishandle personal information
- Persistent identity hack or theft

HOW CAN BLOCKCHAIN HELP FOR DECENTRALIZED IDENTITY?

1. Creation of Unique DIDs
2. Storing all the DIDs in the immutable ledger
3. Notarizing all the credentials
4. A security protocol for the DIDs
5. Smart Contract execution
6. Access Consent and Rights

USE CASES OF DECENTRALIZED DIGITAL IDENTITIES



CREATED BY 101BLOCKCHAINS.COM

Source: https://101blockchains.com/digital-identity/

W3C Decentralized Identifiers (DID)

A globally unique identifier that does not require a centralized registration authority because it is registered with distributed ledger technology (DLT) or other form of decentralized network.

Goal	Description
Decentralization	Eliminate the requirement for centralized authorities or single point failure in identifier management, including the registration of globally unique identifiers, public verification keys, service endpoints, and other metadata.
Control	Give entities, both human and non-human, the power to directly control their digital identifiers without the need to rely on external authorities.
Privacy	Enable entities to control the privacy of their information, including minimal, selective, and progressive disclosure of attributes or other data.
Security	Enable sufficient security for relying parties to depend on DID documents for their required level of assurance.
Proof-based	Enable DID controllers to provide cryptographic proof when interacting with other entities.
Discoverability	Make it possible for entities to discover DIDs for other entities, to learn more about or interact with those entities.
Interoperability	Use interoperable standards so DID infrastructure can make use of existing tools and software libraries designed for interoperability.
Portability	Be system- and network-independent and enable entities to use their digital identifiers with any system that supports DIDs and DID methods.
Simplicity	Favor a reduced set of simple features to make the technology easier to understand, implement, and deploy.
Extensibility	Where possible, enable extensibility provided it does not greatly hinder interoperability, portability, or simplicity.

Source https://www.w3.org/TR/did-core/
W3C Working Draft 22 June 2020

W3C DID Example

A DID is a simple text string consisting of three parts, the:

1. URL scheme identifier (did)
2. Identifier for the DID method
3. DID method-specific identifier.

A simple example of a decentralized identifier (DID):

did:example:123456789abcdefghi

A DID URL with a 'service' DID parameter

did:foo:21tDAKCERh95uGgKbJNHYp?service=agent

A DID URL with a 'version-time' DID parameter

did:foo:21tDAKCERh95uGgKbJNHYp?version-time=2002-10-10T17:00:00Z

Source https://www.w3.org/TR/did-core/
W3C Working Draft 22 June 2020

W3C DID Example

The example DID above resolves to a DID document. A DID document contains information associated with the DID, such as ways to cryptographically authenticate the DID controller, as well as services that can be used to interact with the DID subject.

Minimal self-managed DID document


```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }],
  "service": [{
    "id":"did:example:123456789abcdefghi#vcs",
    "type": "VerifiableCredentialService",
    "serviceEndpoint": "https://example.com/vc/"
  }]
}
```


Source https://www.w3.org/TR/did-core/
W3C Working Draft 22 June 2020

W3C Verifiable Credentials ecosystem

DID is a component of larger systems, such as the Verifiable Credentials ecosystem.

W3C Verifiable Credent In the physical world, a credential might consist of:

Information related to identifying the subject of the credential (for example, a photo, name, or identification number)

Information related to the issuing authority (for example, a city government, national agency, or certification body)

Information related to the type of credential this is (for example, a Dutch passport, an American driving license, or a health insurance card)

Information related to specific attributes or properties being asserted by the issuing authority about the subject (for example, nationality, the classes of vehicle entitled to drive, or date of birth)

Evidence related to how the credential was derived

Information related to constraints on the credential (for example, expiration date, or terms of use).

A verifiable credential can represent all of the same information that a physical credential represents. The addition of technologies, such as digital signatures, makes verifiable credentials more tamper-evident and more trustworthy than their physical counterparts.

Holders of verifiable credentials can generate verifiable presentations and then share these verifiable presentations with verifiers to prove they possess verifiable credentials with certain characteristics.

Both verifiable credentials and verifiable presentations can be transmitted rapidly, making them more convenient than their physical counterparts when trying to establish trust at a distance. ials ecosystem

Source https://www.w3.org/TR/vc-data-model/
Verifiable Credentials Data Model 1.0. Expressing verifiable information on the Web
W3C Recommendation 19 November 2019

W3C Verifiable Credentials ecosystem

Holder - A role an entity might perform by possessing one or more verifiable credentials and generating verifiable presentations from them. Example holders include students, employees, and customers.

Issuer - A role an entity performs by asserting claims about one or more subjects, creating a verifiable credential from these claims, and transmitting the verifiable credential to a holder. Example issuers include corporations, non-profit organizations, trade associations, governments, and individuals.

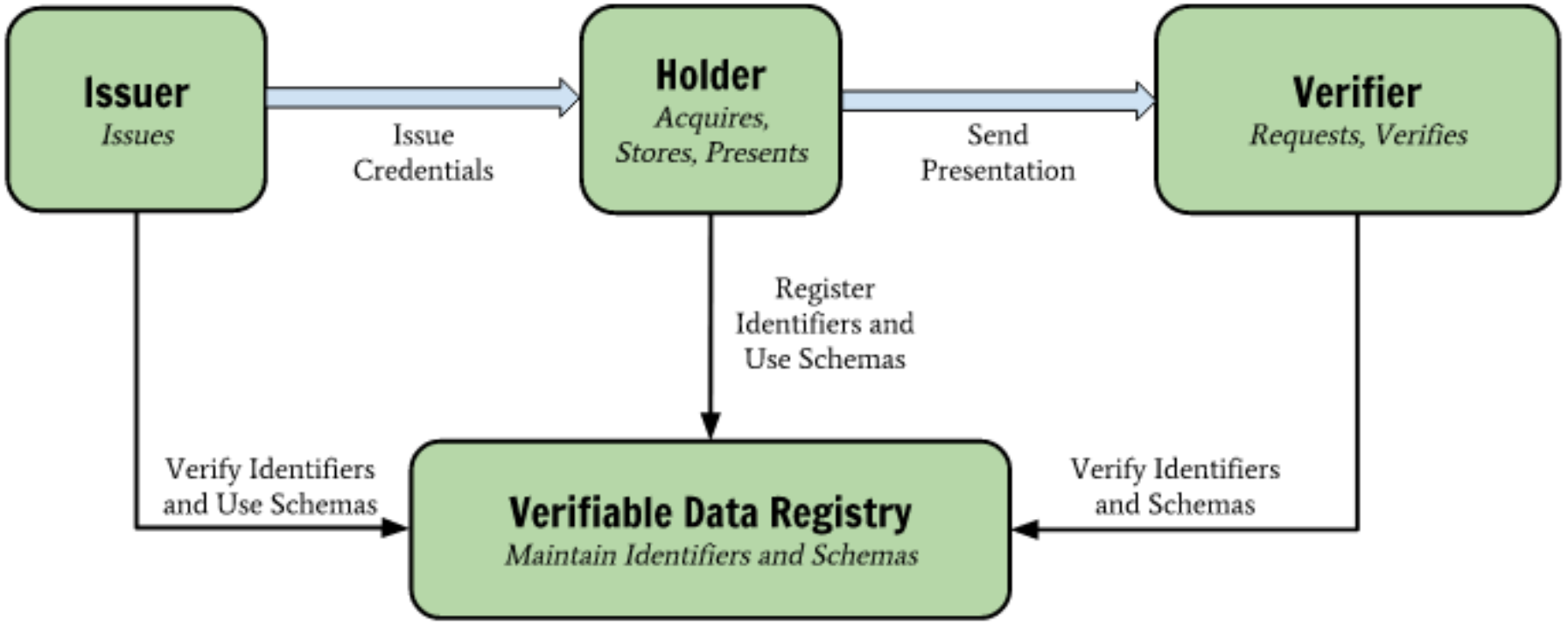
Subject - An entity about which claims are made. Example subjects include human beings, animals, and things. In many cases the holder of a verifiable credential is the subject, but in certain cases it is not. For example, a parent (the holder) might hold the verifiable credentials of a child (the subject), or a pet owner (the holder) might hold the verifiable credentials of their pet (the subject).

Verifier - A role an entity performs by receiving one or more verifiable credentials, optionally inside a verifiable presentation, for processing. Example verifiers include employers, security personnel, and websites.

Verifiable data registry - A role a system might perform by mediating the creation and verification of identifiers, keys, and other relevant data, such as verifiable credential schemas, revocation registries, issuer public keys, and so on, which might be required to use verifiable credentials. Some configurations might require correlatable identifiers for subjects. Example verifiable data registries include trusted databases, decentralized databases, government ID databases, and distributed ledgers. Often there is more than one type of verifiable data registry utilized in an ecosystem.

Source https://www.w3.org/TR/vc-data-model/
Verifiable Credentials Data Model 1.0. Expressing verifiable information on the Web
W3C Recommendation 19 November 2019

W3C Verifiable Credentials ecosystem



Source https://www.w3.org/TR/vc-data-model/
Verifiable Credentials Data Model 1.0. Expressing verifiable information on the Web
W3C Recommendation 19 November 2019

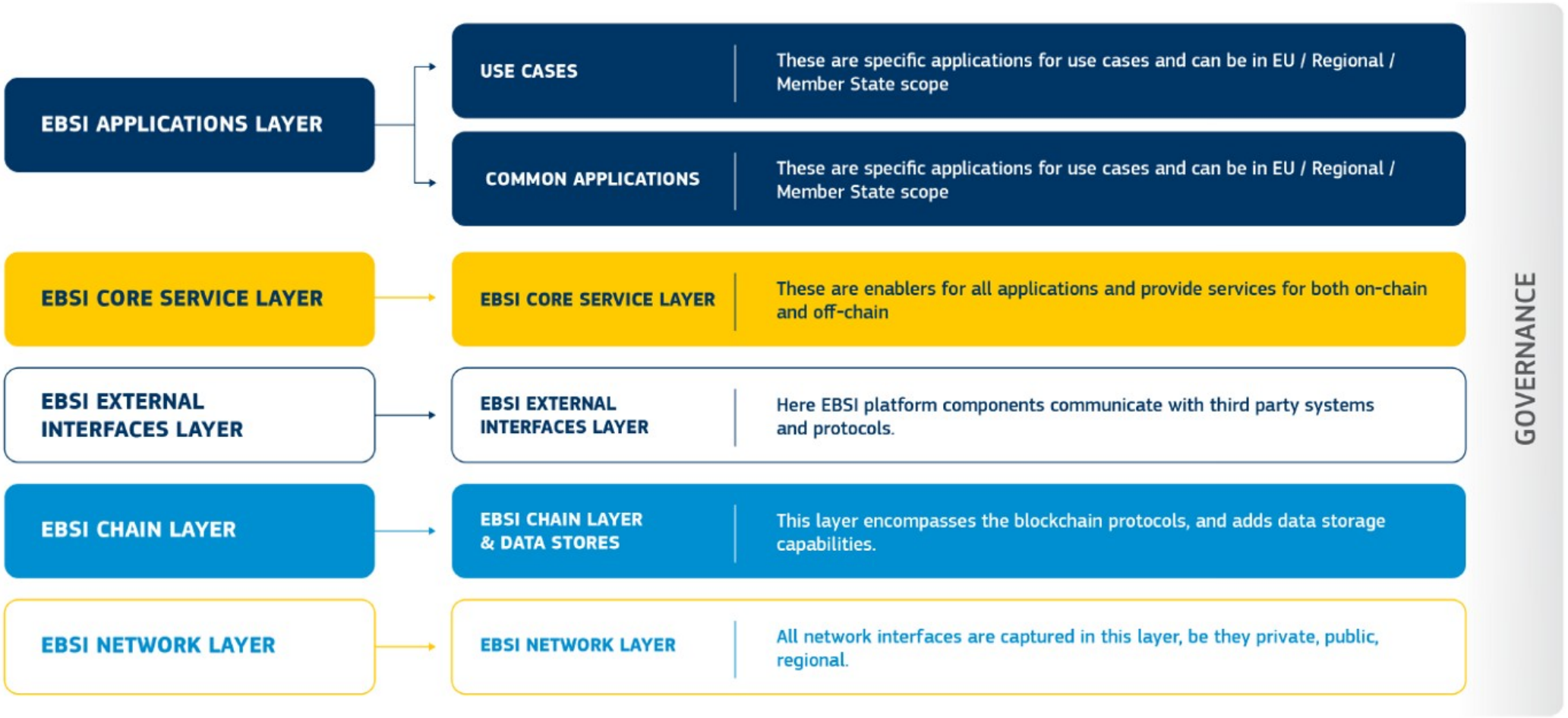
ESSIF: The European self-sovereign identity framework

The European self-sovereign identity framework (ESSIF) is part of the European blockchain service infrastructure (EBSI). The EBSI is a joint initiative from the European Commission and the European Blockchain Partnership (EBP) to deliver EU-wide cross-border public services using blockchain technology.

The EBSI aims to become a “gold standard” digital infrastructure to support the launch and operation of EU-wide cross-border public services. It is a multi-blockchain network with multiple use-cases such as notarization of documents, ESSIF, certification of diplomas and trusted data sharing. While there is an EBSI wallet, it’s for test purposes only and not for the public. The consensus of the permissioned network will be achieved via proof of authority (POA) with one note per member state. The architecture can support multiple protocols and currently is mainly based on Hyperledger.

https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI

ESSIF: The European self-sovereign identity framework



ESSIF: The European self-sovereign identity framework

The EBSI guiding principles are as followed:

PUBLIC PERMISSIONED — The identity of all participating nodes is known

DECENTRALIZED — Each member state should run its own set of nodes

SCALABLE — Support for high-throughput and high number of nodes

OPEN — (Preferably) open-source

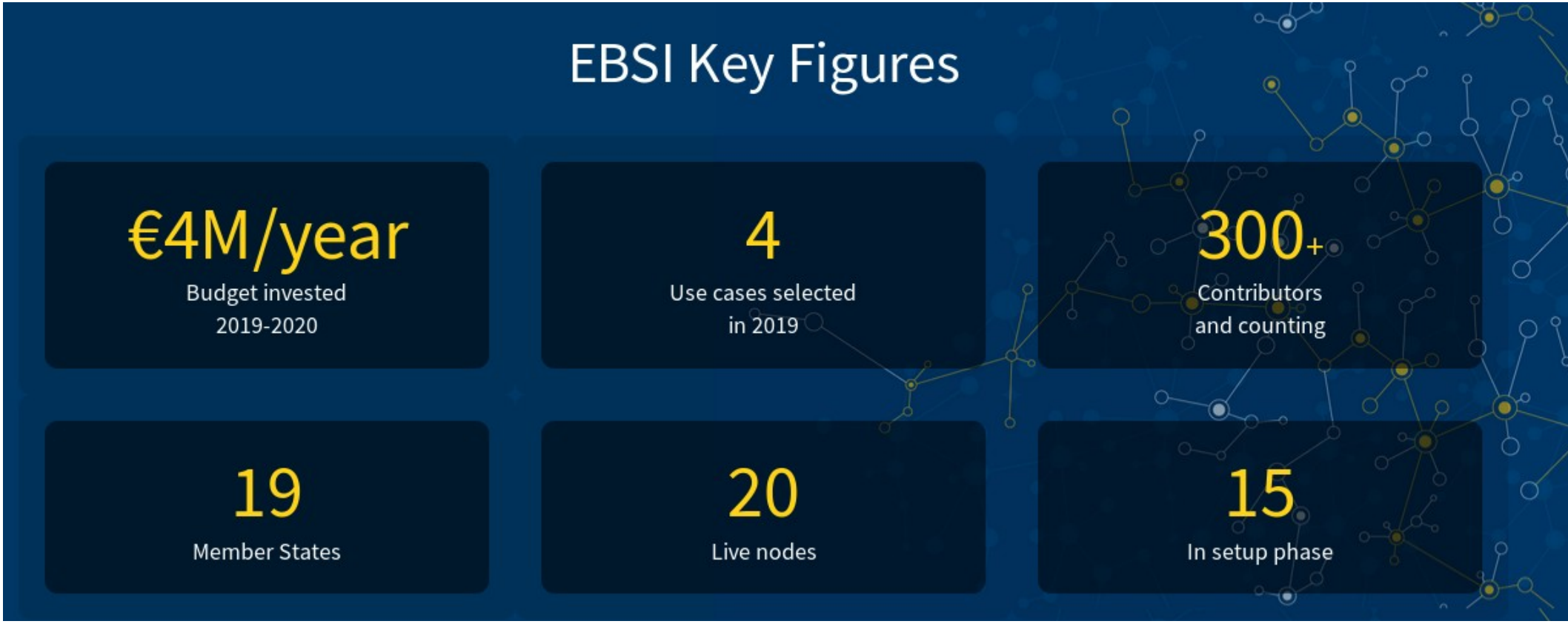
SUSTAINABLE — Energy efficient (Proof of Authority consensus)

INTEROPERABLE — The EBSI should, as much as possible, be based on well-known standards and technical specifications

The goals of ESSIF:

- Provide seamless cross-border services for citizens
- Help make institutions more efficient
- Facilitate economic activity flow across borders

ESSIF: The European self-sovereign identity framework



Source https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI

China Launches National Cryptocurrency and Blockchain Based Service Network (BSN)

The ultimate objective of the BSN is to become the internet of blockchains.

A permissioned blockchain framework **does not have the characteristics of being decentralized and transparent**; rather, all business attributes are formulated by the application owner, and users are required to seek approval from the application owner before they are able to use the application.

At the moment, the BSN already supports Hyperledger Fabric and other consortium blockchain frameworks currently being adapted, including Fabric with Chinese SM2/SM3 Encryption Algorithm, FISCO, BCOS, CITA, XuperChain, Wutong Chain
and Brochain. In regard to public blockchain frameworks, BSN currently supports Ethereum and EOS.

Source https://global.bsnbase.com/

Please read their whitepapers!

Microsoft Patent Published: Cryptocurrency system using body activity data

Some exemplary embodiments of the present disclosure may use human body activity associated with a task provided to a user as a solution to“mining” challenges in cryptocurrency systems. For example, a brain wave or body heat emitted from the user when the user performs the task provided by an information or service provider, such as viewing advertisement or using certain internet services, can be used in the mining process. Instead of massive computation work required by some conventional cryptocurrency systems, data generated based on the body activity of the user can be a proof-of-work, and therefore, a user can solve the computationally difficult problem unconsciously. Accordingly, certain exemplary embodiments of the present disclosure may reduce computational energy for the mining process as well as make the mining process faster.

Source https://patents.google.com/patent/WO2020060606A1/en

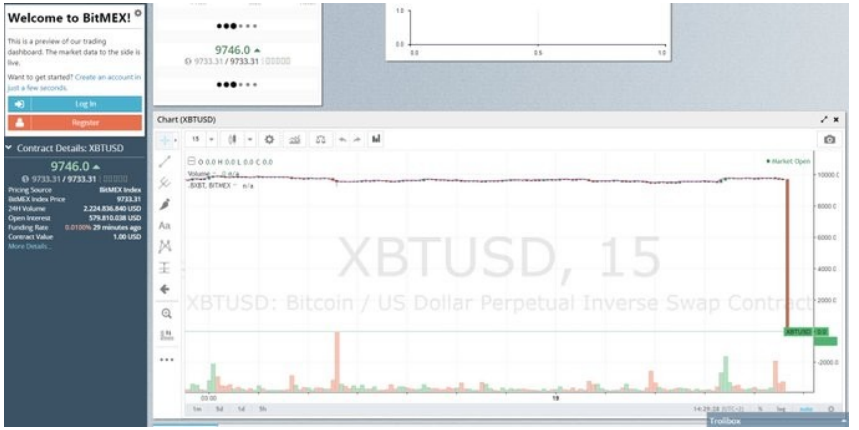
BitMEX Failure

BitMEX exchange technical failure drops Bitcoin/USD pair to zero price: https://www.fxstreet.com/cryptocurrencies/news/btc-usd-bitmex-goes-offline-scares-traders-with-000-quote-for-xbtusd-202005191348

Both website and API of the exchange were unavailable.

The exchange has been stopped to fix the bug in trading engine.

«We’re working to bring the BitMEX platform back online as soon as possible. All funds are safe, delayed orders will be rejected, and no liquidations will occur during downtime. There will be a cancel only period on coming back online.»



https://twitter.com/BTC_JackSparrow/status/1262722198491615235

Information about Cryptocurrency Exchange and Stock Market development and operation funding

Cryptocurrency and trading systems development expert with 12 years experience, Sergey Mereutsa:

«The development cost is starting from $500k USD, 1+ year work for 6-10 person team.»

«The Liquidity investment to fill the Depth of Market starts from $10M USD. And the Exchange will not even be in top 100.»

«Trading Platforms and Stock Market engines are usually written in C/C++/Rust. Java is rarely used as JVM it not always predictable due to GC and Java may decide to perform its memory keeping operations unexpectedly.»

«Stock Market speculations are not directly related to Blockchain because internal trading transactions are inside the engine and are not on the Blockchain and only input and output from the exchange are done via Blockchain transactions programmatically.»

Links

https://101blockchains.com/digital-identity/

https://www.w3.org/TR/did-core/

https://www.w3.org/TR/vc-data-model/