universa.io

Universa Blockchain Platform

v1.0g
prepared_for_universa_corporation_ltd
08_sep_2017

WHITEPAPER

TABLE OF CONTENTS

SYNOPSIS

Abstract.

> “The future is already here —
> it's just not evenly distributed yet.”
>
> — William Gibson 1993, cyberpunk sci-fi author

Distributed cryptographic ledgers back digital currencies exceeding a cumulative $140 billion in value, at the time of writing. Modern cryptography finally protects over half of all web traffic in the form of HTTP+SSL (invented 1995), according to a Q1 2017 report by the Mozilla Foundation. Mathematically-backed asymmetric encryption is provably safe, freely available, and at long last, widely adopted by the overwhelming majority of digital services that impact and empower day-to-day life for most people alive on Earth today.

Over 40 years of computing advancement history has shown that earliest adopters of technologies tend to be hobbyists, followed by consumers, who are followed by businesses, and finally governments. In this regard, as quickly as digital assets like Bitcoin and Ethereum have taken the hobbyists by storm, and are now penetrating consumer wallets, businesses and governments alike are much slower to adapt and adopt. While some brave speculators are already betting their full life savings on these currencies, many businesses still won't yet take them as payment, and most governments do not even acknowledge their status as “money”.

In these regards, cryptographic ledger “blockchain” technology can still be considered in its infancy; the now-famous 2009 whitepaper by the pseudonymous Satoshi Nakamoto describes only the first iteration of a hypothetical use-case, the digitization of money into a trustless and decentralized protocol. The second major iteration on this novel concept yielded Ethereum, a platform and virtual machine far beyond just a currency, supporting complex Smart Contract logic and a new frontier of distributed applications, or “dApps”. Neither is yet fully suitable for enterprise use cases where a degree of regulation and accountability is required.

And thus these two applications are only the beginning of a new age in human communication and cooperation. Blockchains have already begun to disrupt the transmission of monies and the execution of software logic, but the ways they will change business logic and governmental process remain almost completely unexplored. It is a field wide open, ripe for innovation and the pioneering of new systems that will form the basis of how commerce, business and governance occur at a global scale, shaping societies and human culture in the coming years, decades and far, far beyond. The future is indeed here.

Overview.

Universa Platform is a new generation of blockchain technology. It uses a contract execution machine and distributed state ledger designed to improve on Bitcoin and Ethereum technologies by delivering improvements that are imperative for business adoption, with an emphasis on tokenization and contractual agreements. Where traditional blockchains transact primarily in currencies, Universa is designed to support token representation of everything from passports to boarding passes, bus tickets or taxi fares; they can be gift cards, vouchers, or gym membership cards. You might make a token representing your title deed, or just the keys to the house.

While traditional blockchains record a full trustless ledger of all actions, transactions and their effects on a network (“fat protocol, tiny logic”), Universa improves speed and usability by maintaining an directed graph of the verifiable hashes of the output of all actions (“tiny protocol, fat logic”). In other words, instead of stacking blocks to make a single full ledger, each set of changes to a contract is applied by the clients in a separate contract chain (“C-Chains”) to the previous state, and the outcome is vectorized and hashed – only a signed signature of the state of each side-chain gets updated as the new status of the blockchain, discarding the old state and storing the new one. Still, each chain keeps it's own history, and any node with a copy of the transactions can attempt to replay them and verify that the outcome is the same, which ensures validity and fairness in a trusted environment.

In a business-critical derivation from traditional blockchain technology, Universa does not rely on untrusted actors from the general public. Nodes in the Universa

system are owned and operated by our partners; they must be licensed and authorized by Universa Corporation. They are trusted, trained, and audited; they provide guarantees of availability, speed, and security. Rather than mining for incentive – a wasteful activity which needlessly consumes gigawatts of power across the globe every hour yielding nothing – instead all nodes are rewarded via transaction fees for their participation in the validation and execution of contracts. The only "work" being done on the machines in the Universa cloud is mission-critical data handling and contract execution, and does not require expensive GPU hardware. Sensitive business data is not stored flippantly and unwittingly in unknown reaches of the globe, it is encrypted and regulated by strict organizational security practices (ISO 27001, 27002) making it finally possible for enterprises to trust a blockchain with sensitive or private business processes.

What It Does.

Universa Platform is powered by the Universa Network – a swarm of Universa Core nodes composing the Universa Blockchain, and supporting the Universa Secure Signed Document Service (codenamed "Notary Cloud"). The Blockchain is only responsible for enforcing the validity of the state of transactions, while Notary Cloud acts as a verifiable warehouse for signatures of the original contracts.

For example, if a contract is executed that defines a "token" asset and distributes 1 token to each of 10,000 parties, only the hash-of-the-state of the final balances would be stored and saved onto the full blockchain (about 90 bytes), rather than a full accounting of all ten-thousand transactions and the balances of all user accounts, as is the case in Bitcoin or Ethereum; therefore, any future node connecting to the network would then benefit from over 99.99% size reduction in synchronizing this particular execution from blockchain, and it need only to retain the short hash of the current state at this block height to verify it. Furthermore, since the hashes from each contract are summarized into the master Universa chain via directed acyclical graph (DAG), rather than a naive synchronously-ordered blockchain, it's possible for asynchronous actions from different contracts and replays to occur out-of-order and still yield the same final hashes of global state.

The network is designed in this way, around contracts and their executions – “a transaction” – and each time an action is to be performed, all nodes are transmitted both the current state of the contract and the source of the operation to be performed. The state and the source are verified by hash-sum to be identical to the stored current state of the contract's side-chain (“C-Chains”), the operation is applied, and then the new state is hashed and agreed upon by 90% consensus; after a short period of time (10 days currently), the nodes are free to discard both the contract and the state – their hash sum signatures are stored in the Notary Cloud so later, the original contract can be supplied to the nodes and proven authentic – and only the hashes need be retained by nodes in the swarm. In this manner, the transaction speeds are hugely improved and the size of the blockchain is reduced to just enough information to verify the complete historical ledger. To verify a particular C-Chain, such as in triple-ledger accounting of the validity in a currency-like contract's balances, any actor may retain the contract source and transaction history (requesting, if necessary, that it be verified by Notary Cloud) and replay the actions, comparing the hash to the current value at the present state in the ledger.

IMPLEMENTATION

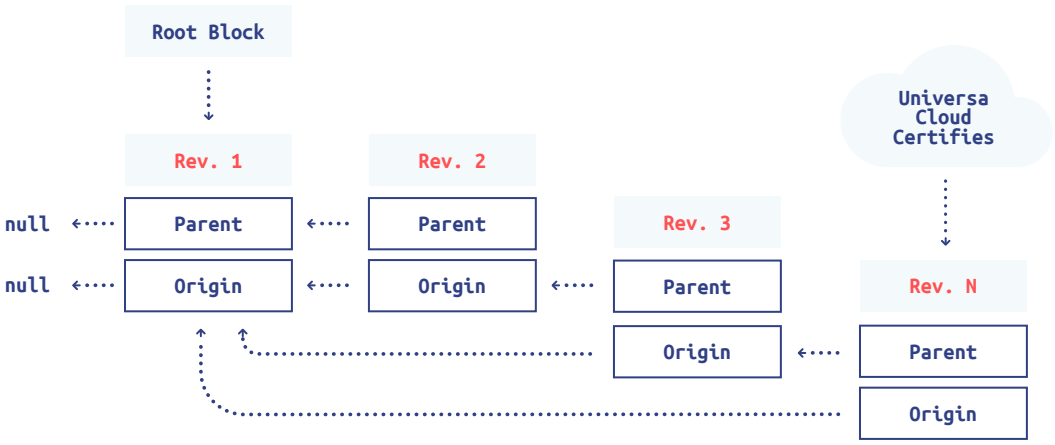
Blockchain.

The Universa blockchain is a cooperative ledger of state changes, performed by licensed and trusted nodes, and is capable of handling thousands or tens-of-thousands of transactions per second (±20,000TPS, http://access.universa.io). It achieves this by performing contract executions on-client and verifying their output by 90% consensus algorithm in the creation of each new block. The blockchain doesn't need to store a full history of all transactions, as these can be kept in the side-chains by each actor responsible for executing them. Anything that would usually be stored in a blockchain on another platform – transaction records, contract sources, and digital signatures – can be later verified for authenticity in the associated Notary Cloud service, which is responsible for handling assets and their digital signatures, but is separate and distinct from the blockchain (which increases transaction speed and synchronization times).

Proof-Of-State.

The Universa Nodes primary function is to execute contracts and verify state. Rather than relying on archaic mining techniques that burn clock cycles for no reason, in Universa, permission to create new blocks comes from participation as a licensed node. Therefore, rather than waiting for a new block to be mined, a state change can occur at any time, verified by a trusted actor, and often approved by consensus in less than ten milliseconds even at scale. Each separate contract maintains its own chain of state, so a contract can perform actions asynchronously without blocking or affecting other contracts, and the combined changes of state collectively form a directed acyclical graph (“DAG”) that makes up the blockchain itself.

Contract Chain



Universa cloud cerifies N^{th} block of the contract chain which certifies the whole chain prior to it.

- root block references nothing
- any block refers its parent and origin
- references are signatures: they also certify the referenced object consistency

Actors.

01

Nodes, which together produce Universa Notary Cloud and Universa C-Chains Ledger

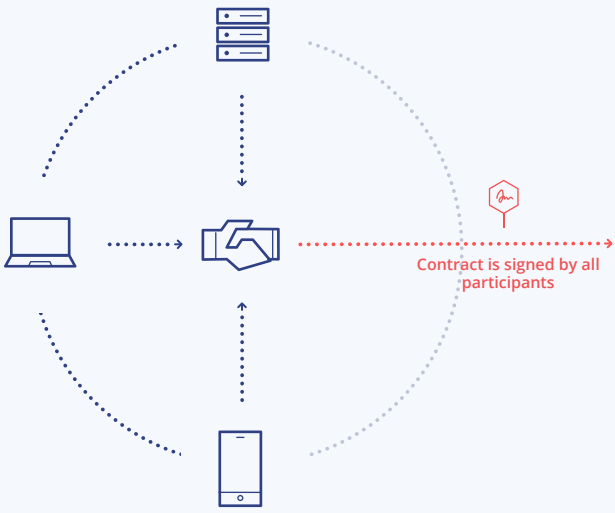
02

Clients – For PC, Mac, Android and iOS

03

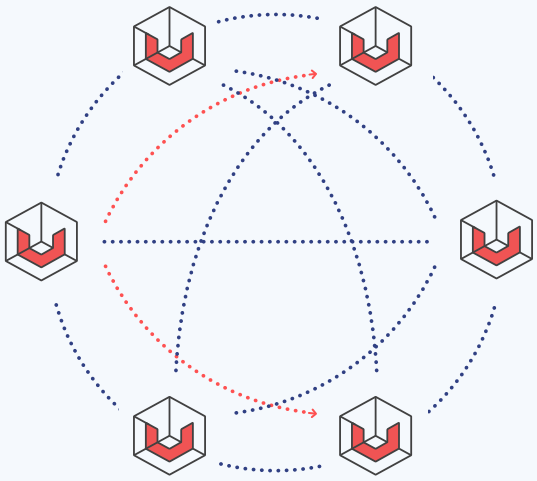
Additional services, like Universa crypto-cloud, and side entities, which will provide services via Universa

Participants Consensus



Slow Consensus
– execution of scripts
– API requests
– verification of files
– calculations of digital signatures

Network Consensus



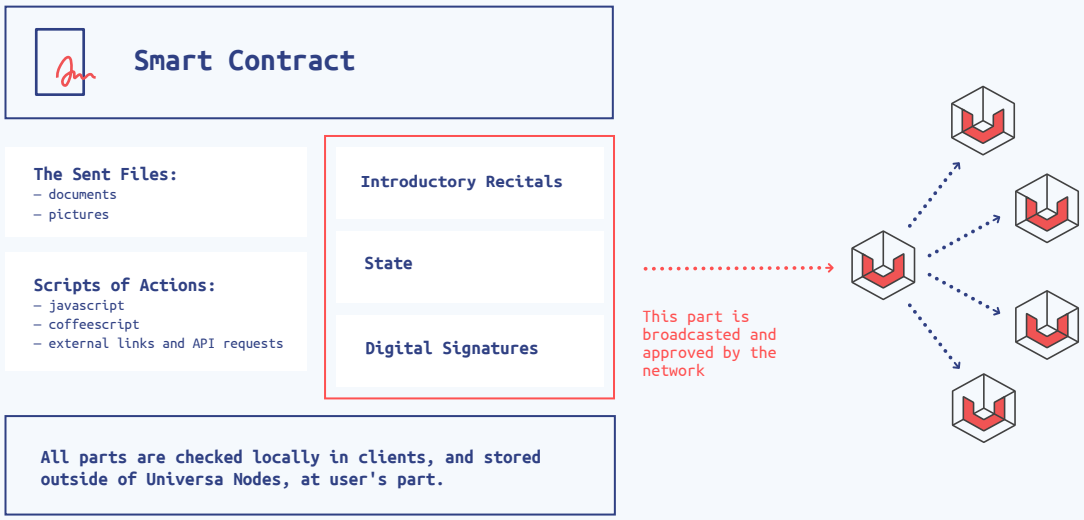
Fast Consensus
– check of permissions
– fast check of digital signatures

Smart Contracts.

In general, a Smart Contract in Universa is just executable script data stored in tree structures. It stores any information in the “key-value” format; each key is represented as a globally unique address, and a value can be fixed values, binary executable logic, dynamically executing scripts, or even references to other trees, addresses, and so on, allowing virtually any structure of complex nesting representations.

Scripts in Smart Contracts in Universa are Turing-complete; put simply, that means that scripts can execute other scripts, and contain programmable logic of significant complexity. In some cases, the appropriate logic to perform a certain action and/or management can be too complicated to be expressed as a set of configuration properties – For example, you might want to associate a share with some external data, e.g, the US dollar exchange rate or a set of stock indices that will allow the share to be sold only under certain circumstances. While it’s almost impossible to include provisions for every possible scenario of this kind in the contract specifications, this could easily be achieved by an executable script stored within a contract. The script is a signed, non-changeable part of the contract that can perform any complex and intelligent logic to check complex conditions, enabling certain triggers and perform further respective actions as needed.

Contract Structure



So, in whole, a tree of smart contracts creates a Smart Contract Chain. It represents a set of smart contracts that reference and confirm each other. A C-Chain represents a real-world set of related documents. Features of each new C-chain are defined by their first, brand-new smart contract. But, once again, the blockchain does not store the contracts themselves, just their current status, the body of the contract is stored in other entities, for example – your flash card, or a crypto-cloud. That also means that you can facilitate your smart contracts accounting by any infrastructure, via Amazon servers or in-house hardware, and since its execution is still signed by you and verified by the node accepting the state of the transaction, its results will still be trusted by all actors in the Universa platform.

Attaching Files.

Smart contracts could include ownership of a real-world object, such as an intellectual property (IP) item included as an attachment, or a contract to purchase some property (usually, another smart contract).

Any files can be added inside a contract themselves, or as a signed-verified link (which prevents changing of the file) for large files. Universa client will check the link's correspondence when executing the SmartContract and after the Notary Cloud will certify the contract and provide a time stamp for it.

Maximum size of a contract is 1 GB.

Time Stamp.

One more important feature of Universa smart contracts is Time Stamp. When a user client has sent the state of a contract to a Universa node, the last one to check and verify that state stores the time when it happened. Since the Notary Cloud executes it within a second, it is possible to understand the exact moment when the contract was verified or rejected by Universa, supporting legal usage of the Universa SmartContracts.

Marker.

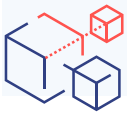
Sometimes you need to have the ability to prove an old status of a smart contract; in case you need to reference a state of a contract at a given point in time, you can create a "marker". This is a special small smart contract, which proves and stores an old state of a needed contract for 2 years.

Nodes.

Each Universa Node is an equal host which stores the structure of the Universa network. Each node is trusted, because it's owned by known responsible owners, legal entities that assume the responsibility for running the notary service. It runs on a regular Unix server and contains a dynamic copy of the ledger. When a client sends a smart contract to a Universa, it is first checked by Universa client which propagates it down the known nodes. If the smart contract is signed only by a few parts, the Universa nodes store its state for 10 days. If the node declines registration of the smart contract, it retains its state for 30 days to prevent fraud.

Clients.

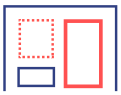
In time, Universa will provide as reference designs and MVPs:



Open source Java libraries, which will work both in desktop environments and on the Android platform

Client application for Windows, MacOS, and Linux, as a command line with basic Universa features set

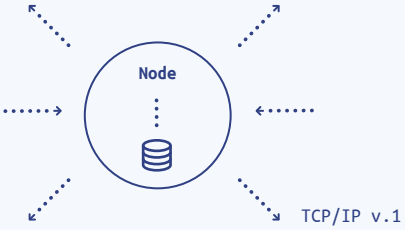
Android mobile application



A Graphical User Interface (GUI) contract constructor, containing templates of contracts and typical actions. The GUI will provide ability to create smart contracts without special technical skills

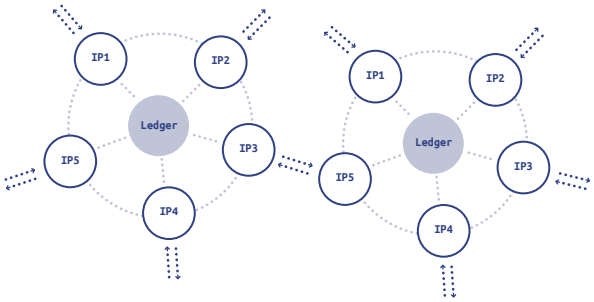
Each type of front-end clients connects with last known nodes and those nodes send to it their lists of other active nodes and the size of quorum. Universa clients always check if an applicant's files are proper for the contract; For example, if you receive documents and a contract via e-mail, the GUI or Universa client will check that this smart contract signatures correspond to the exact versions of the files you received.

Node v.1
August, 2017



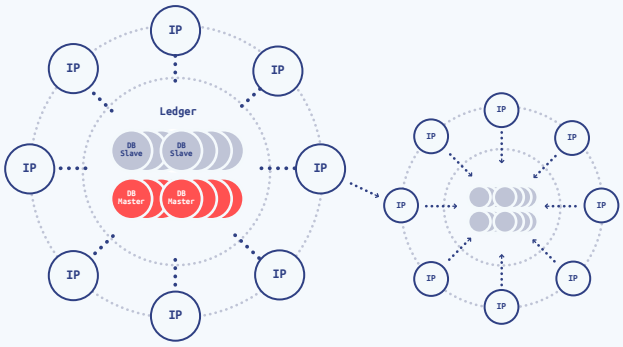
1 x Instance
1 x Ledger
1 x IP

Node v.2
2018, or when daily traffic hits 10M Transactions



3+ x Instance
1 x Ledger
3+ x IP

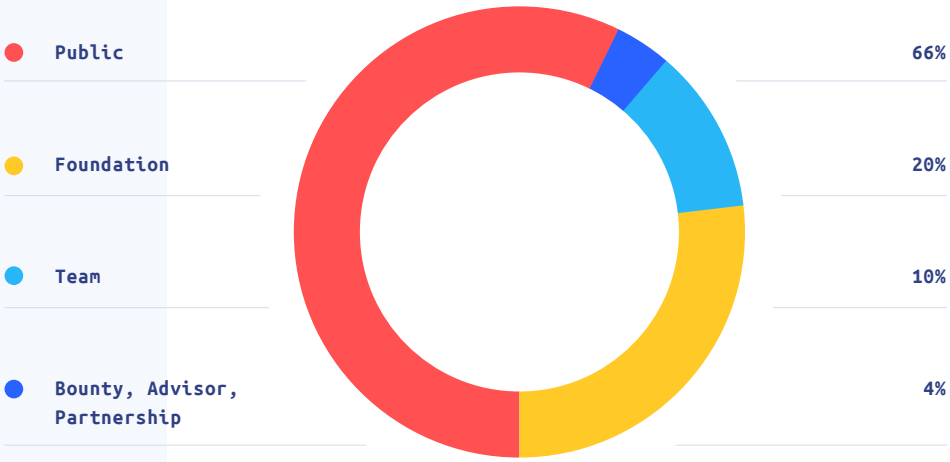
Node v.3
Later 2018 or when daily traffic will be > 100MT



50+ x Instances
1+ x Master ledgers
1+ x Slave ledgers
> 60 IPs
v.2 UDP

TOKEN ECONOMICS

Token Distribution Structure.



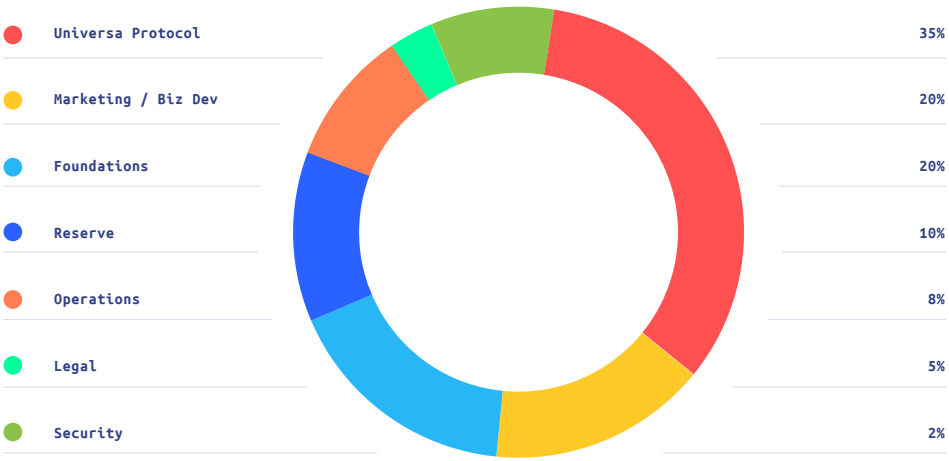
The Universa ecosystem is funded by “UTN” tokens, digital assets that is itself represented as a Universa SmartContract. Each UTN is subdivisible to 18 decimal places, allowing for granular trades. For the sake of convenience and everyday use, nicknames exist for fractional UTN tokens as follows –

UNIT NAME	UTN VALUE	TRADE RATIO	TGE USD VALUE
kUTN	1000	1 : 1,000	$10
UTN	1	1 : 1	$0.01
mUTN	0.001	1,000 : 1	0.001 US cents
uUTN	0.0000001	1,000,000: 1	0.000001 US cents
nUTN	0.0000000001	1,000,000,000: 1	0.000000001 US cents

Pre-Sale and Token Generation Event.

Tokens will be initially distributed in 2 stages, schedule below. During the TGE, an Ethereum “ERC20” token will be generated as a placeholder and distributed to participants, so that placeholder tokens can be traded on open exchanges before the Universa blockchain goes live. Participants can choose either to claim their placeholder tokens immediately via distribution to an Ethereum wallet, or to wait to claim their rewards until after the Universa platform is operational. Tokens will be generated and distributed on the main blockchain at the launch of the Universa Platform. Participants from the TGE and Pre-Sale who did not claim placeholder ERC20 “UTN-P” tokens will be distributed their reward UTN directly; the tokens will sit in a “Placeholder Redemption” account, and holders UTN-P will be able to redeem them in exchange for UTN.

	PRE-SALE SEPTEMBER 2017	TOKEN GENERATION EVENT 28TH OCTOBER 2017
TYPE	Public Offering	Public Offering
KNOW-YOUR-CUSTOMER “KYC”	Required	Required
TOKENS TO SELL	1,000,000,000	–
AMOUNT TO ACCEPT	$3-10 million USD	Up to $99 million USD
PRICE PER UTN TOKEN	$0.01 + 20% bonus	$0.01 (min purchase is $10)



Circulation & Demand.

Execution of Smart Contract actions requires transaction fees paid in UTN to reward participating nodes for the processing power they supply to the network and sustain the ongoing development of the Universa platform. Nodes will keep 80% of the transaction fee, and 20% will go to Universa Corporation. Universa will hold the right to “burn” each day up to 1% of the fees retained by the platform.

All the settlements in a platform will be executed in tokens only, no other methods will be accepted

All the prices will be set in USD (except price for nodes, this can be set in tokens)

During each transaction, actual token rates from the exchange will be used to determine the amount of tokens to pay for each service

All the users need to buy tokens to use platform, and crypto-exchange module in self-service portal will manage automatic conversion of external currencies (and digital assets) to UTN tokens and back

Buy (and keep!) more tokens today - you will ultimately pay less tomorrow for any Universa services

Budget + Spending Plan.

Universa's token generation event is designed to garner financial support from an open crowdsale of partners who want to support our future development. Our plan is dynamic and capable of adjusting to a wide variety of circumstances; we are conservatively prepared for a modest fundraising event and will move forward with our plans, using only the funds contributed in pre-sale even if the ICO doesn't draw another dollar. However, optimistically, our ultimate goals and vision for the project are advanced and we're fully prepared with a plan for scaling the company to $99 million USD and eventual growth beyond. Our ICO is capped at $99 million USD because we aim to disrupt many legal and political frameworks entrenched around the globe and build Universa's Foundation.

A full budget and spending plan, including development goals, legal structure, and research targets, is available for all to browse at http://bit.ly/2fkELHm

FUNDING AMOUNT	CURRENT	$5M	$10M	$25M	$50M	$75M	$99M
STAFF HEADCOUNT	17	17	25	30	35	40	45
DEVELOPMENT	$2,167,500	$2,167,500	$3,187,500	$3,825,000	$4,462,500	$5,100,000	$5,737,500
RESEARCH	$0	$0	$400,000	$900,000	$2,000,000	$5,000,000	$7,000,000
MARKETING	$0	$400,000	$800,000	$1,200,000	$2,000,000	$5,000,000	$7,500,000
LEGAL	$250,000	$400,000	$400,000	$800,000	$800,000	$2,000,000	$2,000,000
BUSINESS DEV	$0	$250,000	$600,000	$1,200,000	$2,400,000	$3,000,000	$4,000,000
EDUCATION	$0	$200,000	$400,000	$1,000,000	$1,500,000	$2,500,000	$3,000,000
YEARLY BUDGET	$2,417,500	$3,417,500	$5,787,500	$8,925,000	$13,162,500	$22,600,000	$29,237,500

Additional Services.

Service providers can register as a regular server, with active Universa smart contracts. There is nothing special from “Universa” point of view, as the nodes will behave like typical blockchain participants, but they can provide custom interactions to extend the functionality of the network and deliver advanced capabilities.

For example, a contract could incorporate a set of API calls to external services to allow and/or perform actions and to generate results. A public share contract can have an endpoint that performs “vote” action for its owner by specifying a GET or POST HTTP request to a given URL, or an endpoint to generate dividends as e-currency emitted by an e-bank service.

Universa will provide, either at launch time or shortly thereafter, reference implementations of several common use cases for SmartContracts in the Universa Platform. These reference implementations will be open source and adaptable, allowing anyone to directly copy them, or to use them as a basis for future developments. References will be provided for “Tokens”, “Invoices”, “Escrows”, and “Organizations”.

Token Contracts.

Common Tokens.

The most basic example use of SmartContracts will be in the generation of a common Token asset. Such assets can be divisible, tradable, and are fungible; the contract will define actions to check the balance of a wallet, and to transfer tokens to another wallet; in this way, Universa Platform can host a wide variety of tradable assets for powering other platforms and trades. More advanced token contracts might contain functions for minting new tokens, burning existing supplies, freezing or locking trading activities of one account or all accounts, and issuing authorizations for spending by an intermediary party.

Bank-Backed Tokens.

Because SmartContracts are fully Turing-complete and can interact with external APIs, it is possible to define a Common Token Contract that includes extra provisions for handling transfers to-and-from an externally defined asset class, including but not limited to Bitcoin, Ethereum, or even fiat currencies. For example, a contract might define a token called “USD-TETHER" and support an integration with a US bank account, and define a function “sellTokensToFiat", which accepts USD-TETHER coins to be burned and a SWIFT address as input, and triggers an outgoing wire to the corresponding bank account. Conversely, a corresponding “buyTokensWithFiat" action could be defined that mints new USD-TETHER coins upon receipt of an inbound wire transaction. Such a contract might similarly be used to back Universa assets with other digital assets, as well, allowing full interoperability with external funding methods via the Universa Platform.

Invoice Contracts.

For example, you are the boss of any offline services firm, and you would like to receive payments for your service instantly after delivery and with small transaction expenses. You create a smart contract with all documentation in appendix and conditions, and stipulate that your customer should send USD-TETHER tokens as remuneration; the contract can be defined to specifically forward the assets directly to the manager's account, or to your accounts receivable department. When your workers provide delivery, your staff ask the customer to provide his digital signature for that action to a terminal and the transaction will be executed immediately. This action can even be made offline and registered on the network later. If necessary, before signing the contract you can send its body to each other for negotiations, but when one side signs it with official digital signature it becomes an immutable document, and another side will be able only to sign the completely same contract or not to sign that contract at all.

Escrow Contracts.

Digital Exchanges or “Stock Markets”.

Similar to how Bank-Backed Tokens might leverage external APIs to allow the trade of other digital or fiat assets, a SmartContract can be defined to provide a trustless escrow lock of a two-party transaction to release a trade when both sides have posted their payments. In this way, the exchange can facilitate crypto-to-crypto trades, or even integrate with a stock broker service to allow other kinds of securities to be traded, using UTN, fiat, or another digital asset as payment.

Selling an Apartment.

First, the seller should prepare a smart contract with a package of documents, that confirm his property. It can be images of paper documents about his property, that are signed with his legal digital signature and, in some countries – by notary also. That should allow to change the owner in exchange for a defined bank token, in this case for example 250,000 of the above-defined USD-TETHER token.

Now both sides can negotiate and revise the contract. After signing the contract by both sides one of them sends it to any node of Universa. Universa checks all signatures and ensures the sufficient presence of 250,000 USD-TETHER tokens. If the contract passes the verification by 90% of nodes it is executing, the buyer receives the right of possession of the apartment, and the seller becomes the owner of the bank note token. Now the buyer can connect with local authorities or registration departments to send them documentation about the new apartment owner.

Digital Autonomous Organization “DAO” Contracts.

You are the CEO of one firm and are organizing voting about new CFO. First, you create a smart contract, which describes your proposition of the new CFO, their rights and duties in all common nuances of a standard legal document. After that, you press the button “Start voting” in your GUI. Next, you send the contract to your involved colleagues via any channel – even by flash card and your legs. Participants launch the contract, prove their identity and rights to vote with their digital signature and vote. Each vote creates another new, separate smart contract with the vote of a person, as previously defined in the main smart contract. After, these persons send their “Vote” contracts to you. After you receive enough of such contracts you will be able to update your main corporate smart contract with a new CFO; the smart contract is an element of digital workflow infrastructure, and because it contains the paperwork as attachments, it represents a fully legal document at the same time. The smart contract allows the new CFO to bill entities and pay salaries, and is suitable for presentation in the court and government tax service.

CONCLUSION

Universa Platform iterates cryptographic ledger technology, building on eight years of proven Bitcoin success in the distribution of money and adapting it with the tools needed to address fundamental business concerns and governmental compliances. With transaction throughput improved by several orders of magnitude, built-in support for verifying document authenticity, and a network of trusted certified nodes, Universa is able to provide necessary usability to open new avenues into enterprise adoption. As consumer needs are increasingly served by rapid advances in Bitcoin and Ethereum technologies, Universa will continue to lean into blockchain adoption and leverage distributed innovations to serve the reliability and security demands of corporations.

universa.io