Decentralized Apps, Smart Contracts, Value Transfer, & Self-Governance Protocols on a Distributed Application Ledger

Abstract: Proof of Stake algorithms promise significant advantages in achieving distributed consensus compared to Proof of Work. Combining Proof of Stake with other important requirements, such as the automation of cross-organizational collaboration with mobile wallets that support simple payment verification (SPV) techniques and others, will allow for broader industry adoption. Moreover, having an existing user friendly infrastructure that allows digitalization and self-governing tokenized ecosystems is essential to achieve a global adoption. These self-governing ecosystems must have complete autonomy on top of the blockchain via the development of fully scalable sidechains. Ethereum, the leading smart-contract platform of the first decade of blockchain technology's existence, is facing scalability issues due to its computationally expensive Proof of Work algorithm & the necessity for nodes to download the entire blockchain which limits the utility of the Ethereum blockchain. This white paper introduces the Eureka smart contract framework that aims for sociotechnical application suitability insuring long term scalability and reliability as well as interoperability with the other blockchains. The Eureka Blockchain is powered by Eureka Coin (ERK). The coins will be continuously bought back and burned using the net profits of the development company Polaris Universal until the total circulating supply of the coin is 10 Million ERK. The purpose of this buying and burning process is to insure a decent level of price stability in the long term. 10% of the transaction fees will be continuously burned and this is an in-built feature of the Eureka blockchain. The open source decentralized platform supports the use of SPV solutions in addition to allowing for diverse implementations of fully autonomous sidechains. The blockchain comes with a complete infrastructure that allows building, storing, and trading self-governing PoS-based tokens. Eureka is a state of the art blockchain built to be widely used for industry-cases applications.

1. Introduction

Smart contracts are computer protocols that facilitate, verify, and enact negotiated agreements between consenting parties. These contracts allow the performance of credible transactions without an intermediary. This technological breakthrough can allow for a great deal of progress in different domains such as digital-signing solutions [1], Internet of things (IoT) [2], fintech [6], value transfer, storing value, etc. Smart contracts are built on top of decentralized ledgers which need a decentralized validation system through means such as Proof of Work (PoW) [7] and Proof of Stake (PoS) [3]. The core technology that enables smart contracts is called blockchain and it is a decentralized ledger of consecutive blocks that are validated and added to the chain using decentralized nodes. Thus blockchains do not require any third party to run reliably and securely. This technology was first introduced and popularized with the invention of Bitcoin [8], a peer to peer cryptocurrency and payment system. Bitcoin uses PoW for block validation, meaning that nodes use computationally expensive equipment to do the validation.

Bitcoin allows a limited set of operations to be done on top of its protocol. On the other hand, many decentralized ledgers use the Turing-complete language Solidity (which resembles the JavaScript syntax), the latter allows the enactment of smart contracts, e.g., Ethereum Virtual Machine (EVM) [9]. By the time of this writing Ethereum has proven to be the leading DAPPs and smart contracts platform worldwide despites having multiple problems. The proof of work mechanism of Ethereum limits the scalability options of the network making it realistically unable to handle industry-cases applications. Ethereum faced different security issues throughout its existence; for instance, an Ethereum based decentralized application was hacked recently [10] resulting from a lack in the latest tools required for formal verifications [11]. The hack resulted in a loss of $50 million and Ethereum performed a hard fork in the aftermath of the incident resulting in two separate chains. Later down the road Ethereum performed another hard fork due to a denial of service attack [12]. More future hard forks are expected in the Ethereum blockchain [5].

There are many reasons that limit Ethereum's mass adoption: The inefficiency of the current Proof of Work validation system and the need for more secure and stable virtual machines for blockchains with better performing Proof of Stake transaction validation [3], and the lack of

privacy protecting differentiations between external versus related internal private contracts which makes the cross-organizational information-logistics impossible on the Ethereum blockchain. Furthermore, Ethereum lacks formally verifiable smart contract languages, lite wallets that do not require downloading the entire blockchain, and mobile-device solutions for smart contracts with simple payment verification (SPV) which means clients only need to download the block headers when they connect to a full node [4].

To achieve industry-scalability, a smart contract platform needs to leverage the power of sidechains and unspent transaction outputs (UTXO) [13], as well as being able to achieve compatibility to other blockchain systems such as Bitcoin. Moreover, an adoption of features from the Bitcoin Lightning Network [14] allows efficient scalability via bidirectional micropayment channels. Ethereum has been struggling to achieve worldwide mass adoption due to the reasons mentioned above, and Eureka is built to introduce a decentralized blockchain that is able to offer all the state of the art options that a decentralized ledger can offer in addition to solving the above problems and enabling cross-organizational information logistics to optimize costs and time. Eureka is a blockchain built for mass adoption.

2. The Advantage of Eureka

Eureka is a UTXO-based decentralized blockchain that uses a Proof of Stake (PoS) consensus model in which the creator of the next block is chosen based on the held wealth in the native coin of the blockchain (Eureka Coin) instead of using the metric of hash rate like in the case of Bitcoin's PoW. In PoS, blocks are minted by stakers instead of being mined by miners. As a result, the stakers get rewarded with the transaction and deployment fees (Tx fees) of the network. Note that Eureka Coin has a zero inflation rate meaning there won't be any new coins created with each block and 10% of the Tx fees of each block will be burned while the remaining 90% will be distributed among the stakers. When a coin is burned it means it is completely outside of circulation & nobody has access to it.

Eureka is compatible with the Bitcoin and Ethereum ecosystems and the Eureka Virtual Machine is constantly backwards compatible. The Eureka blockchain employs industry use cases while also aiming at mobile device users. This allows promoting blockchain technology to a wide array of Internet users and therefore widening the decentralization of the transaction validation process in the Eureka ecosystem.

- Consensus Mechanism

Eureka uses a Proof of Stake (PoS) mechanism for consensus management. In the Bitcoin network, miners participate in the verification process by hashing through proof of work (PoW). When the hash value of a miner is able to calculate and meet a certain condition, the miner may claim to the network that a new block is mined. The Block Header varies with each different Nonce. The difficulty of the mining adjusts based on the total hash power of the blockchain network. When two or more miners solve a block at the same time, a small fork happens and the chain splits in two. This is where the nodes need to make a decision as to which block they should accept. In the Bitcoin network, the legitimate chain is the one that has the most proven work attached.

It is worth noting that there are different PoW algorithms out there such as CryptoNightV8, Scrypt11, Equihash, etc. The reason behind launching new algorithms is to prevent the accumulation of computing power by one entity and to ensure that Application Specific Integrated Circuits (ASIC) cannot be introduced into the ecosystem which is something that many in the cryptocurrency community prefer. Eureka chooses PoS for consensus formation.

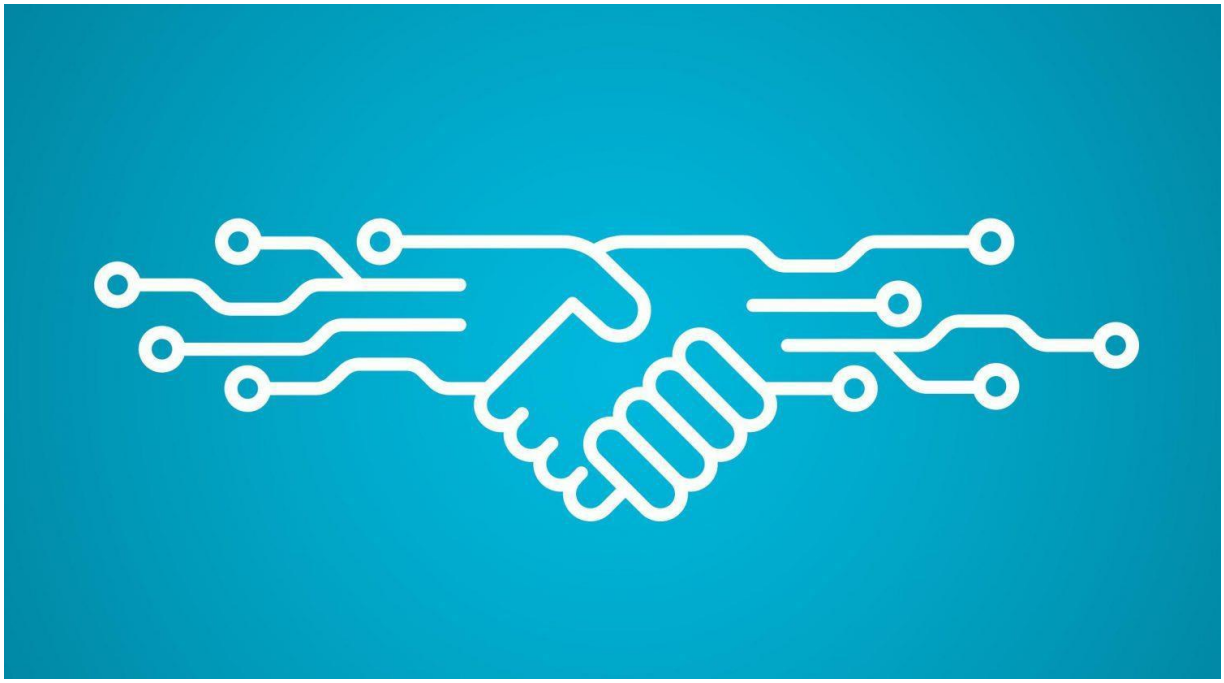
A concept that started the whole idea of PoS was "coin age" which was known to Satoshi Nakamoto as early as the first days of Bitcoin's existence and was used to prioritize transactions on the Bitcoin network. Coin age is simply the coin amount times the holding period. In a simple example, if you receive 100 coins from your friend and hold it for 10 days, it means that you have accumulated 1000 coin-days of coin age. Furthermore, when you spend those 100 coins down the road, we say the coin age that you accumulated with those 100 coins had been destroyed or consumed.
In traditional PoS, the staker pays himself thereby consuming his coin age, while gaining the privilege of generating a block for the network and participating in the Proof of Stake system. The generation of a new block must meet the following condition:

$$\text{ProofHash} < \text{coins} \times \text{age} \times \text{target}$$

The significant problem with this method is that a malicious entity can launch a double-spending attack by accumulating large amounts of coin age. Another problem caused by coin age is that nodes are not

incentivized to stay online after being rewarded. Thus, in the improved version of PoS used in Eureka, coin age removal encourages nodes to be online all the time making the ecosystem much more secure and reliable.

The original PoS implementation suffers from several security issues due to possible coin age attacks, and other types of attacks. The Eureka PoS version rewards stakers who stake their coins longer, while giving no incentive to coin holders who leave their wallets offline.



- Smart Contracts

In Ethereum, smart contracts use the Ethereum Virtual Machine for their execution. The Virtual Machine in Ethereum assumes that the system used to transfer value is the account system, as opposed to the UTXO system. Eureka has a similar Virtual Machine to run smart contracts on top of it, but the difference is that Eureka is based on the UTXO model which is different from Ethereum's account model. The Eureka Virtual Machine is similar in functionality to the Ethereum Virtual Machine. Eureka has an Abstraction Layer that translates the UTXO model to an account-based interface for the Eureka Virtual Machine. This abstraction layer is essential for facilitating interoperability and platform independence.

Transactions in Eureka use the scripting language used in Bitcoin, in addition to the following three opcodes:

- OP_EXEC: Triggers special processing of a transaction and executes specific input Virtual Machine bytecode.
- OP_EXEC_ASSIGN: Triggers special processing such as OP_EXEC and has as input a contract address and the contract data.
- OP_TXHASH: Pushes the transaction ID hash of a currently executed transaction.

Execution and validation happens when a transaction input references the output. The transaction is valid when the input script provides valid data to the output script which returns non-zero.

Eureka allows smart contracts that execute immediately when merged into the blockchain. This is achieved by the special processing of transaction output scripts that contain either OP_EXEC or OP_EXEC_ASSIGN. When one of these opcodes is detected it is executed by all nodes after the transaction is put in a block. In Eureka the script language carries data to the Eureka Virtual Machine.

In order for the UTXO set of the Eureka blockchain to not get too large, OP_EXEC and OP_EXEC_ASSIGN transaction outputs are also spendable. OP_EXEC_ASSIGN outputs are spent by contracts when they send coins or tokens to another contract, or to a public keyhash address. OP_EXEC outputs are spent whenever the contract uses the suicide operation to remove itself from the Eureka blockchain.

The Eureka Virtual Machine is designed to function on an account-based blockchain since the concept is borrowed from Ethereum. Eureka is based on

bitcoin and uses a UTXO blockchain and contains an Abstraction Layer that allows the Eureka Virtual Machine to work on the Eureka blockchain without significant modifications to the Ethereum Virtual Machine and existing Ethereum contracts.

The Virtual Machine account model is simple to use for smart-contract programmers. Operations exist that check the balance of the current contract and other contracts on the blockchain, and there are operations for sending fund and/or messages to other contracts.

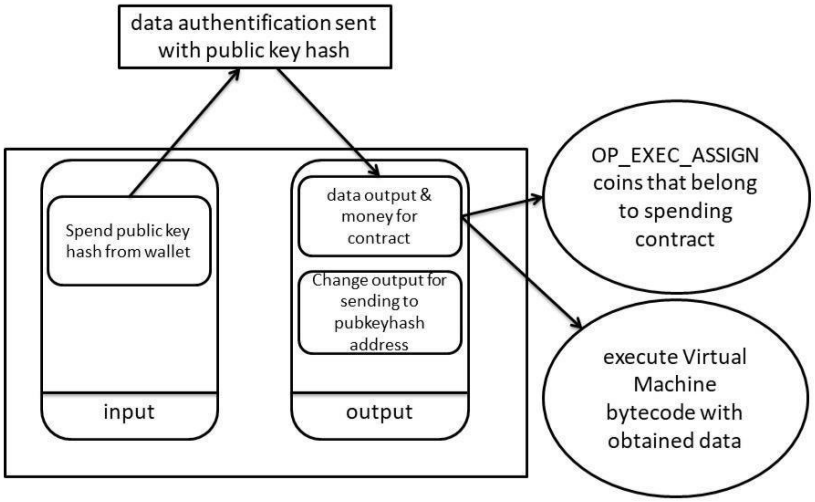


Fig. 1. Contract TX for assigning funds & messages.

The figure above shows the method of sending funds from one contract to another. When the contract sends funds to another contract or public key hash address, the sending contract spends one of its owned outputs and it involves Expected Contract Transactions for the sending. These transactions must be in a block to be valid for the Eureka network. Expected Contract Transactions are generated by stakers while verifying and executing transactions, rather than being generated by consumers, and they are not broadcasted to the Eureka network.

The opcode OP_TXHASH is the mechanism allowing the performance of Expected Contract Transactions in Eureka. OP_EXEC and OP_EXEC_ASSIGN have two different modes. The Eureka Virtual Machine is executed when the former opcodes are executed as part of the output script processing. On the other hand, when the opcodes are executed as part of input script processing, the Virtual Machine is not executed to avoid double execution. Instead, the OP_EXEC and OP_EXEC_ASSIGN opcodes behave similar to no-ops and return either 1 or 0, which translate to "spendable" or "not spendable"

respectively. OP_TXHASH pushes the current spending transaction's SHA256 hash onto the Script stack. The OP_EXEC and OP_EXEC_ASSIGN opcodes check the Expected Contract Transaction list during a spend attempt.

If the transaction passes to the opcodes that exist in the Expected Contract Transaction list, the result is 1 meaning spendable. If not, the return is 0 meaning not spendable. Accordingly, OP_EXEC and OP_EXEC_ASSIGN using vectors of outputs are spendable only when a contract and the Abstraction Layer require that the vector of output is spendable. Note that the contract compatibility between Eureka and Ethereum is strong and very few modifications are required to move an Ethereum contract to the Eureka blockchain.

A management cycle is essential for securing smart contracts and a proper vetting of potential collaborating parties must take place before enactment. Smart contracts have the ability to solve many issues that might occur in the existing cross-organizational models when a business transaction conflict emerges from a contract. The value proposition of the Eureka Framework is the automation of cross-organizational information and value-transfer logistics. The Eureka framework is usable, scalable, applicable, easy to adopt, economically viable, highly automated, flexible, and secure. The smart-contract management cycle is the following: Setup, rollout, enactment, rollback, termination. One of the instrumental concepts to achieve industry adoption is building and maintaining trust in the sociotechnical Eureka system [16] to be reliable in the long term. In this case, trust pertains to the dependencies among humans who use technology to achieve goals. Eureka is economically viable and easy to adopt. The former means that using the Eureka system results in an economic return on investment, while the latter means the barrier of entry for working with Eureka is extremely low.

- UTXO Model

In the UTXO model whenever a transaction occurs, it uses as input unspent coins that are destroyed, and as output the new UTXOs that are created as change and returned to the sender [15]. So whenever a certain amount of coins is transferred among different private keys, new UTXOs are spent and created in the transaction chain. The UTXO of a transaction is unlocked by the private key that is used to sign a modified version of the transaction. In Bitcoin the scripting system processes data by stacks and the developers use isStandard() function [15] to summarize the scripting types. Bitcoin clients support: P2PKH (Pay to Public Key Hash), P2PK (Pay to Public Key), MultiSignature (less than 15 private key signatures), OP_RETURN, and P2SH (Pay to Script Hash).

For example, using P2PKH for the script creation and execution, let's say we're paying 0.01 BTC to someone, the output of this transaction is:

OP_DUP OP_HASH160 <Public Key Hash> OP_EQUAL
OP_CHECKSIG OP_DUP duplicates the top item in the stack.
OP_HASH160 returns a Bitcoin address as top item.

To establish ownership of a Bitcoin, a Bitcoin address is required along with a digital key and a digital signature. OP_EQUAL gives TRUE (1) if the top two items are exactly equal and FALSE (0) if they're not. Then OP_CHECKSIG produces a public key, a signature, and a validation for the signature pertaining to hashed data of a transaction, returning TRUE if a match occurs.

The unlock script according to the lock script is:
<Signature> <Public Key>
The combined script with the above two: <Signature>
<Public Key> OP_DUP OP_HASH160 <Public Key
Hash> OP_EQUAL OP_CHECKSIG

The execution of the script combination is true only when the unlock script and the lock script have a matching predefined condition. It means the Signature must be signed by matching the private key of a valid Address signature and then the result is true. With that said it is worth noting that Bitcoin's scripting language is not Turing-complete meaning there is no loop function unlike Eureka.

The UTXO model allows a great deal of privacy since users can use Change Address as the output of a UTXO. Moreover, in this model it is possible to transparently trace back the history of each transaction through the public ledger. Eureka is UTXO-based for the reasons mentioned earlier, and its blockchain allows implementing smart contracts based on the innovative design of the UTXO model as opposed to Ethereum's account model.

In Ethereum, balance management resembles what a bank account looks like in the real world. Every account has its own balance, storage and code-space base for calling other accounts or addresses, and stores respective execution results. Internal transactions are only visible in the balance of each account and tracking them on the public ledger of Ethereum is a challenge. Eureka is based on the UTXO model which we believe is much better than the account model.

- Gas Model

The gas model is used in Ethereum as the transaction fees' protocol. In order to turn the Bitcoin blockchain into a Turing-complete protocol, there must be a mechanism to determine the fees paid to stakers without relying solely on the size of a transaction. The reason is that a transaction may infinitely loop and cripple the entire blockchain.

Eureka adopts the concept of gas from Ethereum in which the each executed Virtual Machine opcode has its own price and each transaction has an amount of gas to spend. As soon as the transaction is sent any remaining gas is refunded to the sender.

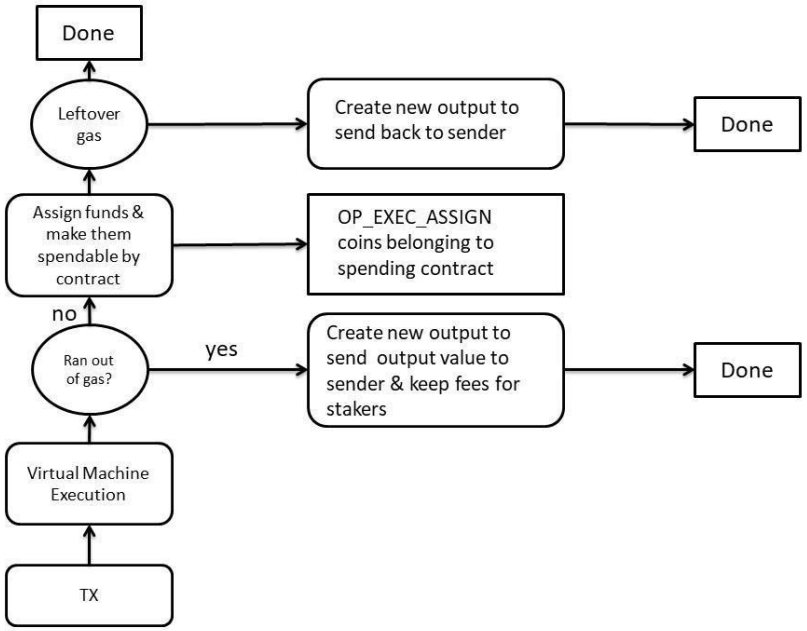


Fig. 2. Gas refund model.

When the required gas for contract execution exceeds the amount of gas available in a transaction, the changes caused by the transaction are reverted. Thus, any modified permanent storage is reverted and the funds are not spent. With that said, all gas of the transaction is consumed and given to the processing staker since the staking resources have already been spent. We expect the the gas price of each virtual machine opcode to be significantly different from Ethereum due to the specifications of the Eureka network as opposed to Ethereum.

When creating a transaction or deploying a contract, the user specifies two things for gas. First is the GasLimit which determines the amount of consumable gas set for the contract execution. The second aspect is the GasPrice which sets the exact price of each unit of gas that the user is ready to pay, and it's given in Yuris which are the equivalents of Satoshis in Bitcoin meaning they are the smallest units that the Eureka blockchain records as fractions of ERK. The maximum Eureka expenditure of a contract execution is equal to the multiplication of GasLimit by GasPrice. If this maximum expenditure exceeds the transaction fee provided by the transaction then the latter is invalid and cannot be processed. The remaining transaction fee after subtracting this maximum expenditure is the Transaction Size Fee and analogous to the standard Bitcoin fee model.

To determine the appropriate priority of a transaction, stakers consider two metrics. First, the transaction size fee must match the total size of a transaction. The second metric is the GasPrice of a contract execution. By combining these two, stakers choose the most profitable transactions to process and include in a block. Consequently, there is a free-market fee model with stakers and users optimizing for the best fee that suits their transaction speed and the price they are willing to pay. It is worth mentioning that the Eureka blockchain is very fast, cheap, and reliable. This is due to the philosophy of combining both on-chain and off-chain scaling solutions and not putting any unnecessary caps that might be scalability bottlenecks to the ecosystem down the road.

3. Sidechains

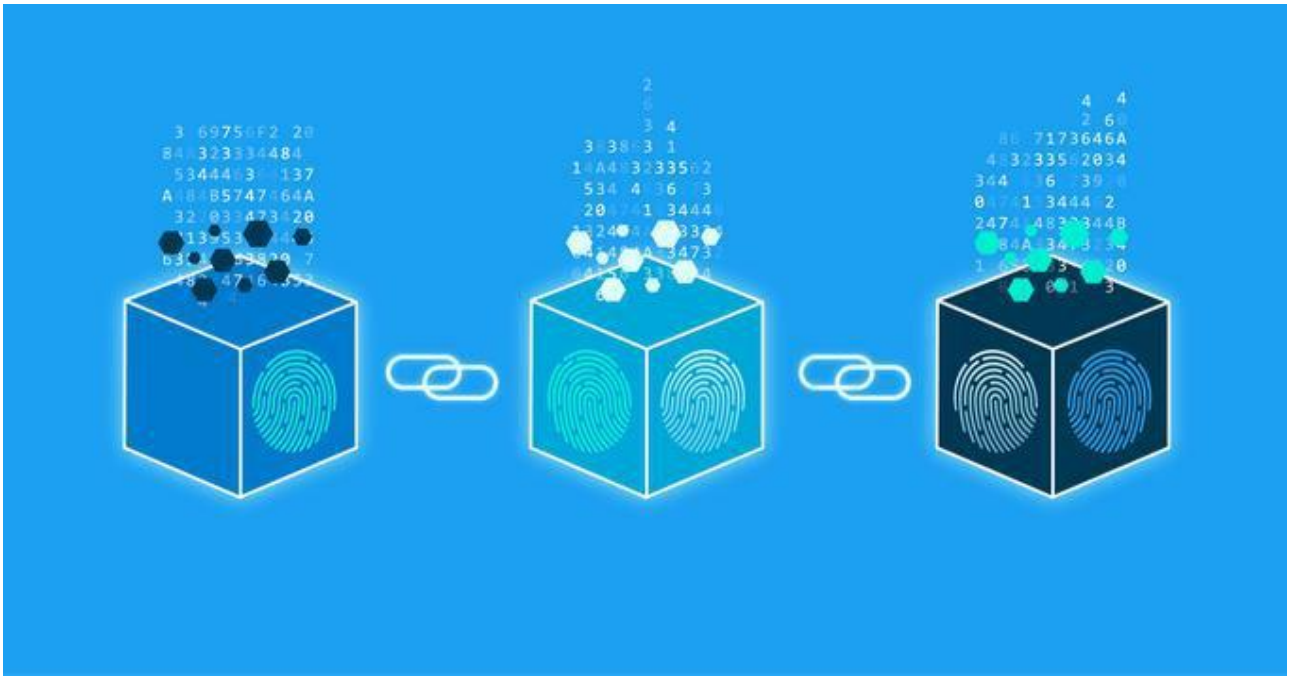
Even though Eureka is built to be able to scale on chain to big levels, having sidechains built on top of the protocol will insure a great deal of efficiency which will help maintain the smooth running of the network at all times. A sidechain is a secondary ledger that runs in parallel to the Eureka blockchain. Entries from the Eureka blockchain can be linked to and from the sidechain; this allows the sidechain to operate independently of the Eureka blockchain. The two main implementations of sidechains that are being developed by Polaris Universal are payment channels and Proof of Stake tokens. The possibilities are endless with sidechains and people from all over the world can build sidechains on top of Eureka. The development company is working on user friendly interfaces that developers can use to build secure and reliable sidechains on top of Eureka quickly. Bitcoin's lightning network is one of the most efficient ways to transact cheaply and quickly across the world. Eureka has all the specifications needed to host lightning-like payment channels. One the other hand, the ability to build PoS tokens will allow developers to build self-governing tokens, and the stakers of the token will receive the transaction fees generated when the tokens are changing hands, in addition to being able to govern the sidechain through nodes. Eureka is an open source blockchain and we expect to see a lot more innovation in the field of sidechains through the next years and beyond, and Eureka is a state of the art open source blockchain that has all the characteristics needed for global adoption.

4. The Infrastructure of the Eureka Ecosystem

Eureka's technology allows for sidechains to be built on top of the protocol. The Eureka blockchain comes with an infrastructure that will insure consistent adoption from the start. A user friendly interface will allow anybody to launch a token, similar to Ethereum's ERC20 standard, which is governed through a separate Proof of Stake mechanism. This means holders of the token will be able to stake their tokens to secure and govern the token's sidechain and collect the transaction fees generated by the token. Note that the transaction fees will be paid using the Eureka Coin since it is the native coin, or fuel, of the primary blockchain. A user can simply head over to the interface and enter the name, symbol, decimals, and total supply of the new PoS token in order for it to be created. The goal of having such interface is to make tokenization and digitalization much more user friendly while also responding to the increasing demand for self-governing tokenized ecosystems.

Eureka also comes with a user friendly wallet to store Eureka Coin and the tokens built on top of the protocol. The same wallet interface will allow coin holders and PoS token holders to participate in Proof of Stake. Furthermore, any token that is created can start trading right away in a Peer To Peer decentralized exchange that is built on top of Eureka which is also a part of the infrastructure that comes with the Eureka blockchain. The development company Polaris Universal is behind this infrastructure that will allow adoption and insure utility from the very early days of Eureka's existence.

5. Eureka Blockchain Economy



- The Concept of Eureka

In the 20th century humanity made an important step towards increasing the quality of living of everyone on earth due to the breakthrough that was achieved in transmitting information globally. After the rise of computers, internet came along to solve a lot of issues and make transmitting information extremely fast and reliable through the TCP/IP protocol. The development of interconnection technology such as Internet, Internet of Things, and Virtual Reality have introduced more diverse ways to interact among people, information and objects, and allowed more things to become digitalized and tokenized. The next evolution that humanity needed at that point was solving the many issues that come with global information-sharing by optimizing security and trust. A key innovation that was needed to start this new generation of technology is some way to share information and value using peer to peer methods. Bitcoin was introduced by Satoshi Nakamoto in late 2008 and came up with the idea that will change humanity forever. Satoshi invented a peer to peer electronic cash system which meant he was finally able to find a way to transfer value and information digitally in a completely secure and decentralized way. Eureka is an extension of this story.

❖ The Background and Significance of the Eureka Blockchain

Eureka uses the technology of blockchain which was introduced with Bitcoin back in 2008. Blockchains are decentralized ledgers meaning there is no single server that's on top of the system and this in turn means there is no single point of failure. This creates extremely secure systems that the world can build its infrastructures on instead of relying on centralized servers which act as single points of failure and the damage can be catastrophic when these servers are hacked. A blockchain is distributed among nodes all over the world and each node acts as a reviewer of the ledger. The effect of decentralization on security is indeed ground breaking. On the other hand, decentralization in itself is a great thing for humanity since it gives people the power to avoid third parties when they are not needed. And whenever intermediaries are not needed, having them forcefully is actually harmful for the wealth of nations. History has been showing us that in many situations intermediaries can develop powers that they are not supposed to have like dictating to people what they can and cannot do with their money, assets, and sometimes their lives. There is no way to insure that those powerful intermediaries share the same moral values of good people, and this is why centralization can be very harmful on the macro level and the only solution is disintermediation. In other words, whenever third parties are not needed, there shouldn't be any third party.

❖ Vision of the Eureka Blockchain

The blockchain industry today still faces many technical and implementation challenges. The main issues are the lack of a new and more capable Smart Contract platforms and the lack of interactions with real world data among other things. We are introducing an entirely new blockchain ecosystem, Eureka, as an alternative option for value transfer protocols in the world. Eureka is based on the UTXO model and uses a Virtual Machine similar to Ethereum's to achieve the compatibility between Bitcoin and Ethereum for public blockchain.

Eureka's goal is to create a globally influential open source community by cooperating with other blockchain communities, third-party developers, and technical innovations. Eureka aims at bringing blockchain technology into the finance, gaming, IoT, social media, and other industries. Eureka is a compatible ecosystem that utilizes Oracle and Data Feeds, in conjunction with the logic of regulation, to bridge the real world to the blockchain world.

We have enough reasons to believe that when the financial damage from centralization is at its peak, people will naturally switch to trading their goods, services, and productive capitals with open source digital currencies. Eureka Coin is a perfect example of a decentralized currency that is built to be able to store value in the long term due to the economic model that is behind it.

- Technical Model of Eureka

❖ Compatibility with UTXO and EVM

We believe that the best blockchain technology that insures consistency of transactions and the traceability of tokens is Bitcoin's UTXO model. On the other hand, all Ethereum's smart contracts can operate on the Eureka blockchain with minimal changes if any. The Eureka blockchain combines the advantages of both Bitcoin and Ethereum networks while addressing all the inherent problems and being interoperable with them.

❖ Consensus

Eureka uses a Proof-of-Stake consensus mechanism which means value is not wasted to external entities and instead kept inside the ecosystem. Bitcoin miners spend billions of dollars to external ASIC manufacturing companies and that is a waste of value that could otherwise be spent on buying Bitcoin itself. In the Eureka case, the stakers need to buy Eureka Coin and hold it in their wallet to participate in the PoS process.

❖ Ledger

The Ledger stores all smart contracts and allows Eureka users to download the codes and contracts in a peer-to-peer network based on their own interests. The Ledger provides transparency, readability, and audibility. Data feeds are the data resources obtained from off-chain. The Oracle selects the most suitable data to trigger the execution of smart contracts, which are stored in a readable format in the Eureka blockchain.

- Data feeds:

Feeds that represent the data obtained from off-chain sources (such as currency exchange rate, stock market, flight schedule, etc.), which are put into the blockchain to execute smart contracts or decentralized applications.

- Oracle:

In Eureka, the oracle could represent a node, a specific trusted organization, an entity, or a public key address. When there are multiple data resources for an inquired data input, the oracle selects the most suitable data resource based on a pre - defined set of rules.

- On-chain and off-chain triggers:

In Eureka, both on-chain and off-chain factors can be used as a trigger to execute smart contracts.

- Eureka Coin

Eureka Coin is the native coin of the Eureka blockchain and it is the fuel of the protocol. Buying the coin is required to be able to send a transaction or to deploy a smart contract, a DAPP, or a sidechain on top of the decentralized ledger. Eureka Coin is the native utility coin of the Eureka blockchain. Polaris Universal, the development company, owns multiple businesses including a cryptocurrency mining farm and multiple projects both online and offline while also engaging in active trading of financial markets. The net profits realized by the company are used to buy back and burn Eureka Coin until the total circulating supply is 10 Million coins. The goal behind such a process is to stabilize the price of ERK as the ecosystem keeps growing.

The total supply of Eureka Coin is 150 million Coins. Eureka Coin is the fuel that powers the Eureka blockchain in addition to having all the characteristics of a solid store of value.

The 2019 Eureka Coin Sale

Number of Coins offered for sale	125 million Eureka Coins
Coin distribution	Each sale will give 10% affiliate commission to the referrer. If the coin buyer is not referred by anybody, the 10% commission will be immediately burned. 15 million Coins will go to the development team and early backers. 10 million Coins will go to the Eureka Foundation. All unsold coins will be burned at the end of the coin sale
The price of 1 Eureka Coin during the Coin sale	$0.05 USD
Accepted Cryptos during Coin sale	Bitcoin (BTC), Bitcoin Cash (BCH), and Ethereum (ETH)

Disclaimer

Participants in the Coin sale are given access to Eureka Coins. The purchaser understands that there is neither expressed nor implied warranty with Eureka to the extent permitted by law, and that Eureka Coin is purchased on an “as is” basis. Purchasers also understand that Eureka will not provide any refund under any circumstance.

6. Conclusion

This whitepaper introduces the Eureka framework for a state of the art blockchain technology solution. Eureka uses Proof of Stake validation and a virtual machine similar to Ethereum's. The latter constantly remains backwards-compatible. Eureka borrows the concept of UTXO from Bitcoin.

The integration of PoS into Eureka constitutes a considerable saving of computational effort over the Ethereum alternative that still uses Proof of Work. Also the use of UTXOs allows a significantly greater deal of scalability compared to the account management of Ethereum. In combination with simple payment verification (SPV), the development company is already building smart contract mobile device solutions for Eureka to achieve mass adoption. The Eureka framework comes with a complete user friendly infrastructure that allows creating, storing, and trading Proof of Stake tokens in addition to creating and building fully autonomous self-governing sidechains. Eureka is a scalable and reliable decentralized blockchain built for business use. More information about the latest updates and developments can be found on the Eureka website.

References

1. N. Emmadi and H. Narumanchi. Reinforcing immutability of permissioned blockchains with keyless signatures' infrastructure. In Proceedings of the 18th International Conference on Distributed Computing and Networking, ICDCN '17, pages 46:1–46:6, New York, NY, USA, 2017. ACM.
2. Aafaf Ouaddah, Anas Abou Elkalam, and Abdellah Ait Ouahman. Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT, pages 523–533. Springer International Publishing, Cham, 2017.
3. I. Bentov, A. Gabizon, and A. Mizrahi. Cryptocurrencies Without Proof of Work, pages 142–157. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.
4. D. Frey, M.X. Makkes, P.L. Roman, F. Ta¨ıani, and S. Voulgaris. Bringing secure bitcoin transactions to your smartphone. In Proceedings of the 15th International Workshop on Adaptive and Reflective Middleware, ARM 2016, pages 3:1 –3:6, New York, NY, USA, 2016. ACM.
5. https://bravenewcoin.com/insights/casper-plasma-and-sharding-a-light-on-ethereums-scaling-spectrum
6. O. Bussmann. The Future of Finance: FinTech, Tech Disruption, and Orchestrating Innovation, pages 473–486. Springer International Publishing, Cham, 2017.
7. M. Vukoli´c. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication, pages 112–125. Springer International Publishing, Cham, 2016.
8. S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.
9. G. Wood. Ethereum: A secure decentralised generalised transaction ledger.
10. https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/
11. K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi, G. Gonthier, N. Kobeissi, N. Kulatova, A. Rastogi, T. Sibut-Pinote, N. Swamy, and S. Zanella-Beguelin. Formal verification of smart contracts: Short paper. In Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security, PLAS '16, pages 91–96, New York, NY, USA, 2016. ACM.
12. https://cointelegraph.com/news/ethereum-hard-fork-no-4-has-arrived-as-dos-attacks-intensify
13. K. Croman, C. Decker, I. Eyal, A.E. Gencer, A. Juels, A. Kosba, A. Miller, P. Sax- ena, E. Shi, E. Gu¨n Sirer, D. Song, and R. Wattenhofer. On Scaling Decentralized Blockchains, pages 106–125. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.
14. J. Poon and T. Dryja. The bitcoin lightning network: Scalable off -chain instant payments, 2015.
15. A.M Antonopoulos. Mastering bitcoin, 2014.
16. E. Paja, A.K. Chopra, and P. Giorgini. Trust-based specification of sociotechnical systems. Data & Knowledge Engineering, 87:339 – 353, 2013.