DAST CHAIN

Decentralized Architecture for Scalable Throughput

Liviu Ionuț Epure

"Anything that can conceive of as a supply chain, blockchain can vastly improve its efficiency - it doesn't matter if its people, numbers, data, money."

BRAILA

2019

Abstract

DAST is a decentralized services platform using complex technology and simple ideas to empower developers, businesses and common people on our way to blockchain technology mass adoption.

There have been several problems on one chain or another defined as “low speed”, “lack of scalability”, “low security” and others. The actual problem is a combination of them all.

These are the main problems of the blockchain.

The more specific problem we were addressing since the beginning is in the advertising industry.

This 200 billion dollar a year industry is full of intermediaries and middlemen exploiting user data and advertising budgets. All the key stakeholders in the value-chain are infected: advertisers with fraud, publishers with their diminishing share of advertising budgets and users with their right to privacy.

Blockchain presents a possible solution to addressing the critical issues in the online advertising supply chain. The question remains whether blockchain scalability, energy efficiency, and token volatility issues can be solved to the extent that online advertising could widely leverage trustlessness and the benefits gained from blockchain technology.

We aim to solve these issues using blockchain technology, keeping user data safe, eliminating middlemen (or most of them), validating leads and highly improving fraud detection and securing publisher payments.

Another problem is that existing payment methods in the Internet of Things (IoT) usually use prepaid cards or mobile devices as the payment medium, which usually needs the user to provide cards, enter password or operate devices and there still is no way of easily using your crypto for day-to-day payments (like simple NFC payments at any POS). Furthermore, these methods also have security flaws caused by its reliance on the third-party financial platform.

And the solution is simple. Basic math combined with logic and a couple of simple ideas to reach a secure, scalable and fast CPoS (Combined Proof of Stake) consensus mechanism with insignificant possibility of misbehavior or error.

This won't guarantee mass adoption, but hybrid smart contracts and services that make the chain wanted and usable for most people will.

So DAST CHAIN is not only a decentralized services platform, but also adds services required for mass adoption, in a package deal.

P.S.: This document is sent to you from DAST Chain, encrypted and with permissions allow from all. If this was a commercial paper we could have set permissions only to authenticated wallets that paid to view/print/edit.

CONTENTS

I. Introduction

2008’s Bitcoin whitepaper was a turning point in the history of money. That’s when decentralized money started.

The next breakthrough was when Ethereum introduced smart contracts to blockchain and DApps and DeFi started to become a real industry.

In 2017, after extensive experience in network infrastructure, web development, programming and affiliate marketing, we started thinking about the idea of DAST. At that time, DAST stood for Digital Advertising and Services Token.

As the acronym says, DAST was supposed to be a token on ERC20 for advertising and services (tracking, fraud detection, smart contracts for advertisers and affiliates and more). The problem was that ERC20 could not support high throughput apps because of the low TPS and high gas fees. So ERC20 was out.

We tried multiple other chains but none could satisfy my project’s requirements.

That is when we started development of DAST CHAIN to be a secure, fast and highly scalable network to support the high throughput myself and others needed.

We studied and combined the best solutions with some innovation and improvement to create a high efficiency Decentralized Architecture for Scalable Throughput and achieved breakthroughs on:

- Fast and secure consensus
- Huge throughput
- Multiple services support
- Native transfers between chains
- Hybrid smart contracts that accept outside data from secure sources

II. Goals

SECURE | FAST | DECENTRALIZED

Staring up, the goal was to create a platform that could support click/lead tracking for affiliate networks and publishers, a platform that can handle fraud detection, make sure publishers are getting paid for their work and affiliate networks pay only for good leads. All this programmatically using smart contracts.

Because the other networks could not handle the required throughput, we started development of a new blockchain. A blockchain that does all that and much more.

It wasn't developed to do much more, just to fit the initial requirements. But the solutions found opened the perspective.

This way, the final goals changed to only one goal. That goal is to achieve a TRUSTED blockchain.

That is achievable by ensuring the following:

- Security
- Transparency
- Speed
- Scalability
- Decentralization

All these were achieved through Decentralized Architecture for Scalable Throughput – DAST Chain.

III. Architecture

DAST architecture is based on a combined consensus algorithm and a scalable architecture without the use of sharding to ensure highest speeds without any loss in security.

The backend of the network consists of nodes that can be builders, validators and witnesses. All the nodes are randomly selected each session for a task, so any node can be a builder, validator or witness, depending on the session label it receives.

To ensure the highest level of security, a minimum of 143 nodes are required to be active at all times. This will allow an unbreakable pool of nodes to choose from for the current session, and will also allow idle nodes to

exchange validated block hash and headers, keeping an index of blocks, positions and locations.

The network also consists of 23 servers that are used for frontend, services, aggregation, hooks, data, leverage, atomic routes, messaging routes.

The servers use DAST Chain technology to interact with DAST Chain, but are not part of the network and do not influence the node network in any way. They are a data aggregator and convertor, to prepare blockchain data for usage and to make it readable.

Data in the DAST Chain is stored in multiple outer/inner index versioned and timestamped databases that sync across the nodes and a versioned indexes database that holds all indexes and is replicating on all existing nodes.

OIIVT decentralized NoSQL databases replicate on block generation on the nodes that hold governance for the current session, and replicate to all the other nodes on Idle Time Notification (ITN).

Replication on ITN ensures resource planning stability and does not interfere with current session block generation, thus decreasing the systems load and used resources.

ITN is a timeframe notification sent by idle nodes. Nodes and their resources are used for block generation only when selected for governance.

VI database has a version number consisting of an unsigned 64-bit integer. At each version *i*, the database contains (iS_i, S_i, I_i) representing initial ledger state iS, last ledger state S and index id I.

Validators can respond to client queries about the ledger history at both current and previous versions and can query a ledger state.

DAST Chain uses the DAST Protocol. A set of links between VI, OIIVT and event blocks form a DAG based on the DAST Protocol. Event blocks contain information on session events, index IDs of previous events and timestamps.

Current RPoS (Reputation Proof of Stake) tagged node can manipulate the VI and arrange indexes based on timestamps.

Witnesses and validators check for authentication on events and for identical transactions. If identical transactions are detected, the one with the smallest timestamp is validated. Event order is arranged by builders.

Also, current RPoS tagged nodes can generate new sidechannels or payment channels, depending on the user's request.

Sidechannels and payment channels handle multiple transactions before adding the final result to the main blockchain. They are tagged depending on their usage and consensus template for each sidechain and payment channel is applied reading the same tag smart contract.

IV. Consensus

DAST Chain uses a somewhat hybrid form of consensus called Combined Proof of Stake (DAST Consensus Algorithm) which is intended to improve speed and security of events on blockchain using the DAST Protocol for distributed ledger technologies.

Consensus is achieved asynchronous and there can be multiple sessions at the same time on the network with different events. Event initiators are connected to the current session and can't join another session until the current one is complete.

DAST's Combined Proof of Stake algorithm consists of Reputation PoS, Delegated PoS and POS. Validators are chosen and labeled for the current session totally random, using a different random function for each label.

For a session to reach consensus, be complete and an event block created it has to be validated by one labeled RPoS, two labeled DPoS, three labeled PoS and three neighbors.

Different from other Blockchain technologies, where the new event block verifies all previous event blocks (including the transactions inside them), all new Event Blocks will verify VI and query OIIVT. A new event block will be connected to its parent event block through hash and all hashes will be derived from parent event blocks and index IDs and will be written in OIIVT that generated another index ID, so that it is impossible to modify or delete the previous event blocks. When an event block is connected, another node will build a new event block on top of that event block.

We rely on an efficiently computable cryptographic hash function, H, that maps arbitrarily long strings to binary strings of fixed length. We model H as a random oracle, essentially a function mapping each possible string s to a randomly generated one and independently selected (and then fixed) binary string, H(s), of the chosen length.

To make the hash secure but not space consuming we set a 256-bit long output. This is short enough to make the system efficient and long enough to make it secure. To find two strings that have the same hash would require 2^{128} trials.

DCA (DAST Consensus Algorithm) provides a probabilistic safety guarantee using multiple random functions to pick from multiple node pools as security parameters. This renders the possibility of a consensus failure arbitrarily small.

DCA is also efficient and green because it consumes a small amount of energy (compared to PoW) and it does so only on nodes that have a role in the current session. The rest of the nodes, when there are no decisions to be made, only consume for db/ledger replication and ITM broadcasts that are unsigned messages. Authentication is done only when the replication starts so the messages broadcasted don’t use bandwidth.

V. Security

To analyze the security of DAST Chain we specify the probability, F, with which we are willing to accept that something goes wrong (e.g., that a verifier set does not have an honest majority).

As in the case of the output length of the cryptographic hash function H, also F is a parameter.

But, as in that case, we find it useful to set F to a concrete value, so as to get a more intuitive grasp of the fact that it is indeed possible, in DAST Chain, to enjoy simultaneously sufficient security and sufficient efficiency. To emphasize that F is parameter that can be set as desired, in the first and second embodiments we respectively set

$F = 10^{-12}$ and $F = 10^{-18}$.

Note that 10^{-12} is actually less than one in a trillion, and we believe that such a choice of F is adequate in our application. Let us emphasize that 10^{-12} is not the probability with which the Adversary can forge the payments of an honest user. All payments are digitally signed, and thus, if the proper digital signatures are used, the probability of forging a payment is far lower than 10^{-12}, and is, in fact, essentially 0. The bad event that we are willing to tolerate with probability F is that DAST's blockchain forks. Notice that, with our setting of F and short sessions, a fork is expected to occur in DAST's blockchain as infrequently as (roughly) once in 1 million years. By contrast, in Bitcoin, forks occur quite often.

A more demanding person may set F to a lower value. To this end, in our second embodiment we consider setting F to 10^{-18}. Note that, assuming that a block is generated every second, 10^{18} is the estimated number of seconds taken by the Universe so far: from the Big Bang to present time. Thus, with $F = 10^{-18}$, if a block is generated in a second, one should expect for the age of the Universe to see a fork

DAST Chain is designed to be secure in a very adversarial model.

A user is honest if he follows all his protocol instructions, and is perfectly capable of

sending and receiving messages. A user is malicious (i.e., Byzantine, in the parlance of distributed computing) if he can deviate arbitrarily from his prescribed instructions.

The Adversary is an efficient (technically polynomial-time) algorithm, personified for color, who can immediately make malicious any user he wants, at any time he wants (subject only to an upper bound to the number of the users he can corrupt).

The Adversary totally controls and perfectly coordinates all malicious users. He takes all actions on their behalf, including receiving and sending all their messages, and can let them deviate from their prescribed instructions in arbitrary ways. Or he can simply isolate a corrupted user sending and receiving messages. Let us clarify that no one else automatically learns that a user U is malicious, although U's maliciousness may transpire by the actions the Adversary has him take.

This powerful adversary however,

• Does not have unbounded computational power and cannot successfully forge the digital signature of an honest user, except with negligible probability; and

• Cannot interfere in any way with the messages exchanges among honest users.

Furthermore, his ability to attack honest users is bounded by one of the following assumption.

We consider a continuum of Honest Majority of Money (HMM) assumptions: namely, for each non-negative integer k and real h > 1/2,

HHMk > h: the honest users in every round r owned a fraction greater than h of all money in the system at round r − k.

Assuming that all malicious users perfectly coordinate their actions (as if controlled by a single entity, the Adversary) is a rather pessimistic hypothesis. Perfect coordination among too many individuals is difficult to achieve. Perhaps coordination only occurs within separate groups of malicious players. But, since one cannot be sure about the level of coordination malicious users may enjoy, we'd better be safe than sorry.

Assuming that the Adversary can secretly, dynamically, and immediately corrupt users is also pessimistic. After all, realistically, taking full control of a user's events should take some time.

The assumption HM Mk > h implies, for instance, that, if a round (on average) is implemented in one minute, then, the majority of the money at a given round will remain in honest hands for at least two hours, if k = 120, and at least one week, if k = 10,000.

Note that the HMM assumptions and the previous Honest Majority of Computing Power assumptions are related in the sense that, since computing power can be bought with money, if malicious users own most of the money, then they can obtain most of the computing power.

But, even if the Adversary would control 50% of the nodes (although this is not a realistic assumption), the chance that his nodes are chosen for validation is negligible.

DAST Chain is likely to be subject to attacks by malicious groups which aim to gain financial profit or to damage the system. Here we explain a few possible attack scenarios and how the DAST Protocol intends to take preventive measures.

Sybil attack

An attacker may make hundreds of chain nodes in a single computer. However, as the node operation method of DAST Chain is using a combination of Reputation Proof of Stake, Delegated Proof of Stake and Proof of Stake the outcome through the voting system will be intended to accurately identify an incorrect node.

An attacker should not obtain an additional vote to add a new node in the network. Also, since a single computer can only create a single node, a Sybil attack should not be possible in DAST Chain.

Parasite chain attack

In a DAG-based protocol, a parasite chain can be made with a malicious purpose, attempting connection by making it look like a legitimate event block. When the Main Chain is created by the builder and the validators under the DAST

protocol, verification for each event block is performed. In the verification process, any block that is not connected to the VI is deemed to be invalid and is ignored, as in the case of double spending.

Transaction flooding

A malicious participant may run a large number of valid transactions from their account under their control with the purpose of overloading the network. In order to prevent such a case, DAST Chain has a minimal transaction fee. Since there is a transaction fee, the malicious user cannot continue to perform such attacks. Participants who participate in nodes are rewarded, and those who contribute to the ecosystem, such as by running transactions, are continuously rewarded. Such rewards are expected to be adequate in running transactions for appropriate purposes. However, since it would require tremendous cost to perform abnormal attacks, it would be difficult for a malicious attacker to create transaction flooding.

VI. Speed

Using the unique DAST Protocol algorithm, DAST Chain solved the issue of scalability with the fast processing of events.

While third-generation blockchain technology might show improved performance compared to previous implementations of blockchain technology, the speed of creating blocks might be still very slow.

DAST Chain ensures high creation and processing performance. So far we managed to reach 5,914 transactions per second on a test network of 53 nodes and low-end configuration (4 cores, 8 to 32 GB RAM, SSD) without the use of sidechains and payment channels.

With a high level of reliability and scalability, DAST believes it is working on a strong third-generation blockchain technology which can be utilized on a large-scale across many domains and industries. DAST chain intends

to not only process large numbers of transactions at scale but also processes event and historical data that can ensure the reliability of transactions.

The DAST Chain, which is based on the DAST Protocol algorithm of DAST, is intended to perform multiple verifications simultaneously, and conduct tests on the directions and validity of transactions at the same time.

As each node can processes transactions that are broadcasted to the DAST network when he is part of a governance session, it provides excellent transaction processing speed. In the past, all participants verified each block sequentially. However, the DAST Protocol algorithm is designed to asynchronously verify and process event blocks in a distributed, concurrent method.

The size of each event block processed by the DCA is intended to be expanded up to 100KB, which DAST believes will be sufficient due to faster block propagation. As an example, assuming that each transaction is 260 Bytes, a single event block can include up to 440 transactions. If the time it takes for each node to create an event block is 0.1 seconds, each node can create 7 to 10 event blocks per second. Assuming that the number of transactions requested is infinite and that 100 nodes are participating, each node would asynchronously and simultaneously create 7 to 10 event blocks per second.

Every time the number of event blocks reaches 2/3 of the entire nodes participating in sessions, the DAST protocol adds and verifies another session. If 100 nodes are available, around 700~1000 event blocks are created per second and are verified at the same time. Since each stage verifies and processes approximately 700 to 1000 event blocks, high performance TPS can be achieved. However, factors such as network latency could reduce TPS.

DAST believes the time complexity of the DAST algorithm means that a much faster performance speed can be achieved.

VII. Scalability

In existing blockchains, all nodes verify and store a single block at a time, leading to longer time in creating blocks and limitations in block size. Therefore, no matter how many nodes are connected, the performance will be limited by the speed of each node. The more transactions require processing, the worse the performance due to bottlenecks on the network itself. Thus, DAST believes parallel approach is required.

DAST Chain is intended to solve the scalability limitations of existing blockchain with the DAST Protocol. This is achieved by adopting a method where few nodes verify the previous transaction by a simple query to the index (VI) and OIIVT, and events are verified and processed asynchronously without being approved by the miners as in prior blockchains. DAST's sidechains and payment channels also increase exponentially the number of transactions per second because the transactions are written to the main chain when all are finalized. Thus, increased transactional load will not lead to delayed approval or bottleneck effects.

Event blocks that store information from transactions that arise include multiple data packages. A data package may include transactions, Smart Contracts, historical information, events, reputation management, and rewards.

DAST Chain intends to make the processing infrastructure in our society more transparent and reliable. With fast and safe processing methods based on DAG and independent management of historical information through "Event Data", the DAST Protocol is intended to be expanded into various industries along with Smart Contracts.

IX. Chain enabled services

We will not talk about money transfers because that is implied. The only thing we can say is that any eDST transfer is almost instant and the fee is negligible.

adaz.cloud - Ads from A to Z and all related services is the purpose of adaz.cloud. It will serve as a direct connection between publishers and advertisers. All connections are based on a real smart contract, each generating it’s own sidechain, and includes DAST chain's tracking, fraud scrubbing, validation and payments. Any advertiser can use preset rules or create their own. Smart contracts are created drag and drop on a intuitive interface, using predefined or custom terms.

Truss is our digital wallet and global payments app. It allows you to hold all your crypto and buy/ sell/ exchange/ send/ receive crypto and fiat. You can also use the app to pay with your phone NFC at any POS around the world and it will be used as authenticator app for SSO with 2FA on all our platforms. The web platform and p2p exchange for Truss is dast.finance.

Dast.dev is our development platform, the interface between us and anyone who wishes to develop apps on DAST CHAIN. It can be used by senior developers and non-developers as well. It features a development environment, sdks, hooks, testing environment, debuggers for any development needs and also an easy-to-use drag and drop interface for smart contracts and most hooks.

We are also developing SDKs for multiple industry branches (like logistics, finance, healthcare, real estate, tourism, digital content, identity, human resources, education…).

X. Conclusions

In this paper, we discussed the architecture of the DAST platform. Compared to other platforms today, which either run classical-style consensus protocols and therefore are

inherently non-scalable, or make usage of Nakamoto-style consensus that is inefficient and imposes high operating costs, the DAST Chain is lightweight, fast, scalable, secure, and efficient. The native token, which serves for securing the network and paying for various infrastructural costs is simple and backwards compatible. $eDST has capacity beyond other proposals to achieve higher levels of decentralization, resist attacks, and scale to millions of nodes without sacrificing security or decentralization.

Besides the consensus engine, DAST innovates up the stack, and introduces simple but important ideas in transaction management, governance, and a slew of other components not available in other platforms. Each participant in the protocol will have a voice in influencing how the protocol evolves at all times, made possible by a powerful governance mechanism. DAST supports high customizability, allowing direct connections to most existing blockchains.

Disclaimer

This document is a technical white paper that presents the current status and future plans for DAST platform and ecosystem of DAST Foundation (DAST). The sole purpose of this document is to provide information, and is not to provide a precise description on future plans. Unless explicitly stated otherwise, the products and innovative technologies organized in this document are still under development and are yet to be incorporated.

DAST does not provide a statement of quality assurance for the successful development or execution of any of such technologies, innovations, or activities described in this document. Also, within legally permitted scope, DAST rejects any liability for quality assurance that is implied by technology or any other methods. No one possesses the right to trust any contents of this document or subsequent inference, and the same applies to any of mutual

interactions between DAST's technological interactions that are outlined in this document. Notwithstanding any mistake, default, or negligence, DAST does not have legal liability on losses or damages that occur because of errors, negligence, or other acts of an individual or groups in relation to this document.

Although information included in this publication were referred from data sources which were deemed to be trusted and reliable by DAST, DAST does not write any statement of quality assurance, confirmation or affidavit regarding the accuracy, completeness, and appropriateness of such information. You may not rely on such information, grant rights, or provide solutions to yourself, your employee, creditor, mortgagee, other shareholder, or any other person. Views presented herein indicate current evaluation by the writer of this document, and are not necessarily representative of view of DAST. Views reflected herein may change without notice, and do not necessarily comply with the views of DAST. DAST does not have the obligation to amend, modify, and renew this document, and is not obliged to make notice to its subscribers and recipients if any views, predictions, forecasts, or assumptions in this document change, or any errors arise in the future.

DAST, its officers, employees, contractors, and representative do not have any responsibility or liability to any person or recipient (whether by reason of negligence, negligent misstatement or otherwise) arising from any statement, opinion or information, expressed or implied, arising out of, contained in or derived from or omitted from this document. Neither DAST nor its advisors have independently verified any of the information, including the forecasts, prospects and projections contained in this document.

Each recipient is to rely solely on its own knowledge, investigation, judgment and assessment of the matters which are the subject of this report and any information which is made available in connection with any further investigations and to satisfy him/herself as to the accuracy and completeness of such matters.

While every effort has been made to ensure that statements of facts made in this paper are accurate, and that all estimates, projections, forecasts, prospects, and expression of opinions and other subjective judgments contained in this document are based on the projection that they are reasonable at the time of writing, this document must not be construed as a representation that the matters referred to therein will occur. Any plans, projections or forecasts mentioned in this document may not be achieved due to multiple risk factors including limitation defects in technology developments, initiatives or enforcement of legal regulations, market volatility, sector volatility, corporate actions, or the unavailability of complete and accurate information.

DAST may provide hyperlinks to websites of entities mentioned in this paper, but the inclusion of a link does not imply that DAST endorses, recommends or approves any material on the linked page or accessible from it. Such linked websites are accessed entirely at your own risk. DAST accepts no responsibility whatsoever for any such material, or for consequences of its use.

This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in any state, country or other jurisdiction where such distribution, publication, availability or use would be contrary to law or regulation.

This document is only available on www.DASTCHAIN.com and may not be redistributed, reproduced or passed on to any other person or published, in part or in whole, for any purpose, without the prior, written consent of DAST. The manner of distributing this document may be restricted by law or regulation in certain countries. Persons into whose possession this document may come are required to inform themselves about, and to observe such restrictions. By accessing this document, a recipient hereof agrees to be bound by the foregoing limitations.

This white paper is an information paper subject to update pending final regulatory review. This

paper does not constitute an offer. any such offer will be subject to final regulatory review and governed by a revised paper and conditions of sale document that will prevail in the event of any inconsistency with the paper set out below. Accordingly, any eventual decision to buy DAST tokens must only be made following receipt of the final paper, and tokens cannot be purchased until the final paper has been issued by DAST when all final regulatory requirements have been satisfied.

This paper is not a prospectus, product disclosure statement or other regulated offer document. It has not been endorsed by, or registered with, any governmental authority or regulator. The distribution and use of this paper, including any related advertisement or marketing material, and the eventual sale of tokens, may be restricted by law in certain jurisdictions and potential purchasers of tokens must inform themselves about those laws and observe any such restrictions. If you come into possession of this paper, you should seek advice on, and observe any such restrictions relevant to your jurisdiction, including without limitation the applicable restrictions set out in the Regulators' Statements on Initial Coin Offerings at the website of the International Organization of Securities Commissions ("IOSCO") (https://www.iosco.org/publications/?subsection=ico-statements). Restrictions are subject to rapid change. If you fail to comply with such restrictions, that failure may constitute a violation of applicable law. By accessing this paper, you agree to be bound by this requirement.