VName

Decentralized address verification system

November 2017

Updated March 14, 2018 - v1.0

VName Team

info@vname.id

Index

Abstract

The cryptocurrency market has shown a vertiginous growth in recent times. Along with the increase in market capitalization, and the number of transactions and individuals actively operating through blockchain wallets and exchanges, there has been a substantial increase in transaction risk.

To mitigate the transactional risk inherent in blockchain-based market dynamics, the VNAME project emerged, which provides a solution that reduces this risk through an innovative verification mechanism.

1. The Cryptocurrency Market

1.1.   Market Capitalization

The cryptocurrency market has been the fastest growing in terms of capitalization[1], a phenomenon that is due to different variables, although it is possible to find three main reasons: (i) new currencies have been created; (ii) its acceptance in the markets has increased; and, (iii) its price against the USD has presented upward trends.

Table 1. Average Market Capitalization of Selected Coins (USD)

Year	BTC Average Capitalization	ETH Average Capitalization
2013	3,031,221,012	-
2014	6,795,850,521	-
2015	3,916,406,000	68,580,520
2016	8,906,762,541	802,015,206
2017	65,861,928,493	20,977,714,553
Jan	14,730,493,548	889,789,613
Feb	17,062,210,714	1,083,868,000
Mar	18,376,880,645	3,033,742,903
Apr	19,492,310,000	4,482,215,667
May	30,476,796,774	11,083,442,903
Jun	43,120,143,333	28,818,780,000
Jul	41,277,312,903	21,196,709,677
Aug	63,067,309,677	27,828,583,871
Sep	67,543,110,000	27,994,546,667
Oct	87,984,983,871	29,128,516,129
Nov	128,228,366,667	33,841,670,000
Dec	254,097,322,581	60,787,638,710
2018	222,001,387,097	106,042,348,387

Source: Coinmarketcap (2018).

---

[1] The capitalization is defined as: [(1 unit of cryptocurrency X its price in USD) = capitalization].

Looking at year-on-year variations, we see that capitalization has grown exponentially, a situation that is even more evident when evaluating the trend of the last six months (August - January), where the capitalization of BTC rose from USD 63B to USD 222B, which implies an increase of 352%. On the other hand, for this interval, ETH presented an increase of 381% in its capitalization, reaching USD 106B. Observing the first data of 2018, it is expected that the capitalization of cryptocurrency will reach historical records on repeated occasions in said year. The increase in terms of capitalization has been accompanied by a greater volume of transactions.

1.2.   Cryptocurrency Transactions

The number of transactions, as well as the volume of these, are of vital importance since they constitute a proxy variable of the real liquidity of the market and the speed at which the cryptocurrency moves in the market. A greater amount of volume in the transactions, as well as a greater number of these are indications of an active and growing market, while a low transactional market and low volume in monetary terms allow to visualize a stagnant market.

The volume of transactions has not been alien to the growing trend of market capitalization. Although this is expected due to the upward variation of cryptocurrency, the volume of transaction has grown in a greater proportion when evaluating variation in the price of currencies.

When considering the constant creation of new cryptocurrencies, the issuance of tokens destined to the financing of new platforms, protocols and systems (among others), and a greater number of entities[2] in the market, it would be expected that the growth of the market will lead to an increase both in the number of transactions, as well as in the volume of these[3].

---

[2] Entities are defined as those individuals, companies or organizations that participate in the market.
[3] From a theoretical perspective, a greater number and variety of instruments that can be valued and exchanged in the market should increase the volume and quantity of transactions. Table 2 shows the monthly increase in the volume of transactions of the selected currencies, the volume of transactions has been accompanied by the creation of new crypto currencies, issuance of tokens and a greater number of entities in the market, which supports the theoretical reasoning.

Table 2. Monthly Transaction Volume of Selected Coins (USD)

| Year	BTC Monthly Transaction Volume	BTC Monthly Variation	ETH Monthly Transaction Volume	ETH Monthly Variation
2017	**869,746,425,900**	-	**271,295,461,040**	-
Jan	5,143,971,700	-	521,748,480	-
Feb	4,282,761,200	-16,74%	467,166,760	-10.46%
Mar	10,872,456,000	153,87%	4,324,810,300	825.75%
Apr	9,757,448,000	-10,26%	3,154,319,700	-27.06%
May	34,261,857,000	251,14%	14,679,954,800	365.39%
Jun	44,478,141,000	29,82%	34,410,801,000	134.41%
Jul	32,619,957,000	-26,66%	31,034,420,000	-9.81%
Aug	63,548,017,000	94,81%	33,197,514,000	6.97%
Sep	55,700,949,000	-12,35%	24,310,300,000	-26.77%
Oct	58,009,358,000	4,14%	13,427,329,000	-44.77%
Nov	140,735,010,000	142,61%	31,904,820,000	137.61%
Dec	410,336,500,000	191,57%	79,862,277,000	150.31%
2018	416,247,860,000	1,44%	163,610,220,000	104.87%

Source: Coinmarketcap (2018).

The number of transactions has increased exponentially. For the second quarter of 2017, the number of BTC transactions amounted to 26,562,054, which implies an average of 291,091 daily transactions. Considering the increases both in capitalization and volume of transactions, it is possible to assume that the number of transactions increased circumstantially for the second half of 2017 compared to the first semester[4].

---

[4] Although we do not have the necessary data to corroborate the trend, supposing that it is upwards in terms of the number of transactions is based on the historical information on the number of transactions, as well as on the variation in terms of market capitalization. and volume of transactions for the second half of 2017.

By having the information regarding the number of transactions and their volume for BTC, it is possible to generate an average transaction value. By assigning an average monetary value to each transaction, a good approximation to the transaction risk[5] was obtained, which amounted to USD 3,332 in the second quarter of 2017.

Graph 1. BTC Quarter Transactions (quantity & average amount)[6]
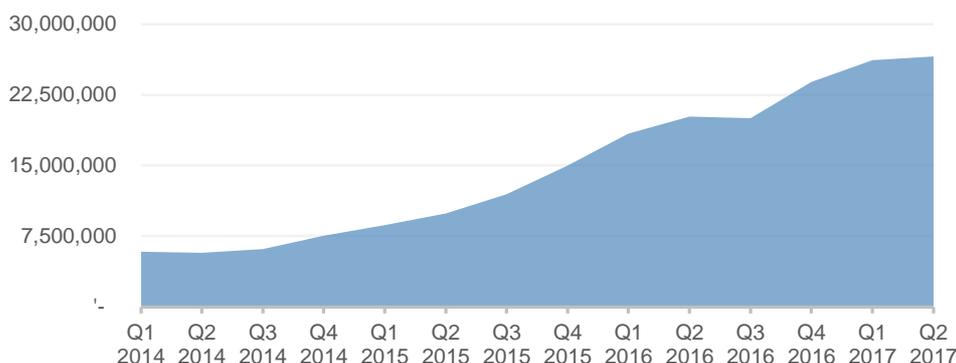
Source: Media Coindesk (2017) & Coinmarketcap (2018).

The increase in the average value of each BTC transaction was 510% between the first quarter of 2014 and the second quarter of 2017. However, the growth was dynamic in the first and second quarters of 2017, where the increase was 122.7% and 330% respectively, based on the previous quarter. As mentioned above, another possible reading would be that when carrying out a transaction in the second quarter of 2017, the risk was 330% higher than making a transaction in the first quarter of the respective year.

1.3.   Blockchain Wallets

Cryptocurrency transactions are performed mainly either through blockchain wallets or exchanges. Using any of the previous options, it also allows the user to monitor their balance, send money and perform other operations.

---

[5] Transaction risk is defined as the monetary value that could be lost in case the transaction does not reach its destination.
[6] The number of BTC transactions made per quarter is found on the primary axis, while the average value of each transaction is found on the secondary axis.

There are different types of wallets, as well as different blockchains. Without delving in the way in which each one works, they can be generalized into those where it is only possible to operate in a single currency[8] or in multiple currencies.

Graph 2. Number Blockchain wallets users
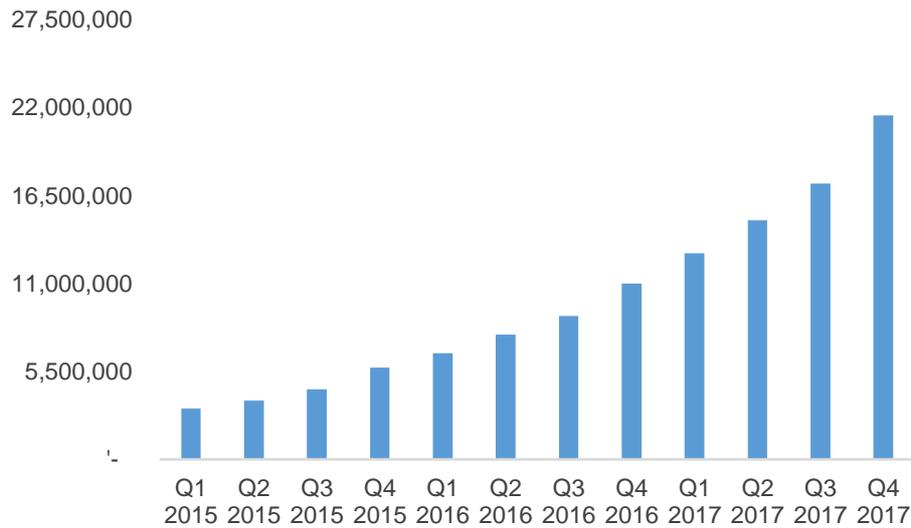
Source: Statista (2018).

In the fourth quarter of 2017, BTC blockchain wallets alone reached 21,506,448 users, which implies an interannual increase of 95.87%, and one of 24.64% compared to the third quarter of 2016.

The number of users of blockchain wallets presents the same trend as the previously analyzed variables. In this way, based on the analysis of the main variables it is possible to conclude that the market is in a process of growth which is expected to accelerate in the near future.

---

[8] Most official blockchain wallets work in this way, there are third party services which allow a user to operate multiple wallets and currencies.

1.4. Cryptocurrency Exchanges

Exchanges are the market agents in charge of carrying out the conversion between the different cryptocurrencies and tokens. Likewise, they have a fundamental role in carrying out transactions operating in different markets. As of 02/24/2018 the volume operated by the 190 main exchanges was USD 5.45B through 6715 commercial pairs.

Observing the ten main exchanges in terms of market capitalization, it is observed that these had an 84% market share with a transaction volume of USD 5.22B.

Table 3. Top 10 Exchanges Marketshare

Rank	Exchange Name	Markets	Trades	Volume (USD)	MarketShare
1	Bitfinex	16	26,237,223	1,843,124,445	30%
2	coinone	6	62,188,405	678,997,924	11%
3	Kraken	56	27,245,852	616,338,160	10%
4	Coinbase	12	17,875,981	616,038,031	10%
5	Bitstamp	11	15,255,358	392,507,648	6%
6	Vaultoro	1	5,979	385,644,365	6%
7	HitBTC	274	101,087,259	199,986,927	3%
8	Bittrex	259	45,972,284	182,522,964	3%
9	Gemini	3	2,592,138	161,266,513	3%
10	Quoine	27	9,061,099	150,693,574	2%
			Total	**5,227,120,551**	**84%**

Source: cryptocoincharts (2018).

1.5. Comments

Cryptocurrency is still part of a new market. Currently, the price of currencies shows significant fluctuations, although with a marked upward trend in the medium term.

When considering fluctuations in terms of contributions, it would be expected that there would be a relationship where the greater the variation of the currencies, the greater the number of transactions. This is because market agents will find incentives to buy and sell not only a greater amount of foreign currencies, but to make a greater number of transactions to reduce losses or invest in future profits.

2. The Problem

2.1. Addresses

The structure of the blockchain implicitly contains a transactional risk. When making a transfer, it is not possible to recover it once it is part of the blockchain. This is a problem because if you transfer to an erroneous address or to a wallet of other currencies, it is not possible to recover the transfer. Also, if that erroneous address did not exist, the crypto-blinds would be lost in the chain and could not be reused, which has an important impact on the chains and generation of value.

As an example, a wallet address of the Ethereum blockchain could be as following: "0x0eb8158424074AEc60f1376ec734a2c0e5f9f735", that is, of forty-two characters based on the hexadecimal system. Making a mistake in just one of the forty-two characters [9] or transferring funds to a wallet that does not handle the currency in question could result in a loss of transferred funds[10].

At present, to carry out transfer between wallets it is necessary to place the address to which the funds are being transferred, and implies a level of concentration not according to the current technological possibilities.

The average Internet user is more familiar with the use of a user name so the use of sequences of many characters goes against the habit and intuition of the user.

With the increasing adoption of cryptocurrency, the user population of it has begun to vary. While initially the main users were those "Tech-friendly" in a moderately homogeneous way, the rapid growth of the market has resulted in a more heterogeneous composition in the users of wallets. It is expected that this will lead to a greater number of human errors at the time of making the transactions and increase the probability of a transaction risk.

---

[9] Considering only lowercase, each character of the directions has 16 possible options, where the probability of writing it correctly is (1/16), since it is forty-two characters, the probability of success would be $(1/16)^{42}$. The figure would amount to a greater number if the permutations were considered. Also, when considering capital letters within the hexadecimal system, each character belonging to the address would be (1/22).

[10] Some blockchains have some kind of address correctness algorithm that would detect invalid addresses and fail the transaction. This is still not enough as sending it to a valid incorrect address is still possible. Moreover, this is considering the verification is even implemented.

2.2. Transactional Risk

After identifying the existing transactional problem, quantifying and measuring the risk of this is of vital importance in order to evaluate the inefficiency and economic-financial loss derived from it.

As mentioned in the market analysis, BTC transactions reached a total volume of USD 88,497,446,000 in the second quarter of 2017[11], while the total number of transactions was approximately 291,091. This implies an average risk of USD 3,332 per BTC transaction.

There are no statistics that indicate what percentage of transactions are lost due to sending them to a wallet that is not appropriate, or due to a typo at the time of putting the address. Given the lack of information, this table is built on different scenarios that between 0.1% and 3% of BTC transactions will be lost.

Table 3. Monetary Loss by Failed Transaction Risk Level (BTC, Q2 2017 in USD)

BTC Transactions	BTC Volume	Monetary Risk (USD)	Failed Transaction Risk	Monetary Loss (USD)
26,562,054	88,497,446,000	3,332	0.1%	**88,497,446**
26,562,054	88,497,446,000	3,332	0.5%	**442,487,230**
26,562,054	88,497,446,000	3,332	1.0%	**884,974,460**
26,562,054	88,497,446,000	3,332	1.5%	**1,327,461,690**
26,562,054	88,497,446,000	3,332	2.0%	**1,769,948,920**
26,562,054	88,497,446,000	3,332	2.5%	**2,212,436,150**
26,562,054	88,497,446,000	3,332	3.0%	**2,654,923,380**

Source: Media Coindesk (2017) & Coinmarketcap (2018).

Under these scenarios, the monetary loss measured in USD derived from BTC transactions for the second quarter of 2017 would be in the interval [USD 88,497,446; USD 2,654,923,380]. It is necessary to make a special mention to three situations:

(i) The estimate is made based on an assumption based on logic. Given the nature of the blockchain, it is not possible to have real statistics regarding the number of failed transactions where users lose their transaction. The assumption is to propose

---

[11] It is noted that in the fourth quarter of 2017 the volume of transactions amounted to USD 609,080,868,000, 588% higher than that observed in the second quarter of that year.

scenarios where it is possible to visualize the expected monetary loss given the number of failed transactions.

(ii)   The values used for the scenarios are from the second quarter of 2017. If the volumes of BTC transactions made in the third and fourth quarter of 2017 are observed, it is possible to appreciate that said volume presented a significant increase, which theoretically would be expected that the monetary loss will be highly superior since the number of transactions should grow more slowly than the volume of these. Given the variant nature of the price of cryptocurrency and the complexity of estimating dynamically, it was decided to use a static situation to assess transaction risk.

(iii)   The proposed scenarios evaluates only BTC. As of February 5, 2018, the volume of transactions of BTC was **50%** of the volume of transactions of the ten main currencies[12]. Considering all the currencies and tokens that are part of the market, the transaction volume of BTC would be significantly less than 50% of the daily volume of transactions. In this way, it is understood that both the number of transactions and the risk associated with them is underestimated considering the entire market.

---

[12] It refers to the ten main currencies in terms of capitalization in the last 24 hours of the mentioned day, these are: Bitcoin, Ethereum, Ripple, Bitcoin Cash, Cardano, Litecoin, Stellar, NEO, EOS and NEM. Source: coinmarketcap (2018).

3. VNAME (NAME) - The Solution

As mentioned in the previous section, the problem is that through the wallets or exchanges withdrawals, it is possible to fail to write correctly the address to which you want to make a transaction. This would involve sending the money to another individual, or a yet non-existent account[13], while on the other hand, the money could be sent to a wallet that does not accept the transferred currency and the amount of the transfer is lost[14].

To solve the difficulty and complexity required to perform a transaction correctly, as well as to minimize the risk associated with transactions, a possible solution is to create a system that facilitates the current transaction mechanism.

This solution should be simple enough as not to disrupt how current exchanges and wallets operate, or how tech-users are already used to transaction. More complex solutions might be implemented with mass adoption.

3.1. Vision

Since the appearance of blockchain, both the cryptocurrency market and its penetration have shown a vertiginous growth. Its expansion has been so dynamic that different issues associated with the ease, safety and use of these have remained unresolved. From VName we believe that by minimizing human error in conducting transactions: (i) it will increase the penetration of cryptocurrency; (ii) there will be a lower loss of efficiency derived from wrongly made transactions; (iii) increase transactional security by having a verification system; and, (iv) the user will feel more comfortable making transactions.

---

[13] Because of how most blockchain wallets work, it is even possible to send transactions to wallets that are valid but have not been created. Once they are created, whoever created it, will have claimed the transaction.

[14] This is even more important in currencies that are forks of others, such as Bitcoin and Bitcoin Cash, or Bitcoin Gold, which have the exact same addresses.

3.2. Objective

Create a mechanism that allows transactions to be easier, faster and safer without compromising user privacy and information. Become the universal access point for validating any blockchain address.

3.3. How does it work?

In simple words, VName works by matching a user's blockchain address to a nickname. A user inputs the destination address of the transaction and our helper script identifies this input and automatically shows the corresponding nickname. The user can, without any modification of their current way of transacting, quickly verify that the receiver of the transaction is indeed who was intended to.

This picture[15] is just a simple demonstration on how VName would integrate with existing sites (e.g. exchanges, wallets). Information and presentation will probably vary.

---
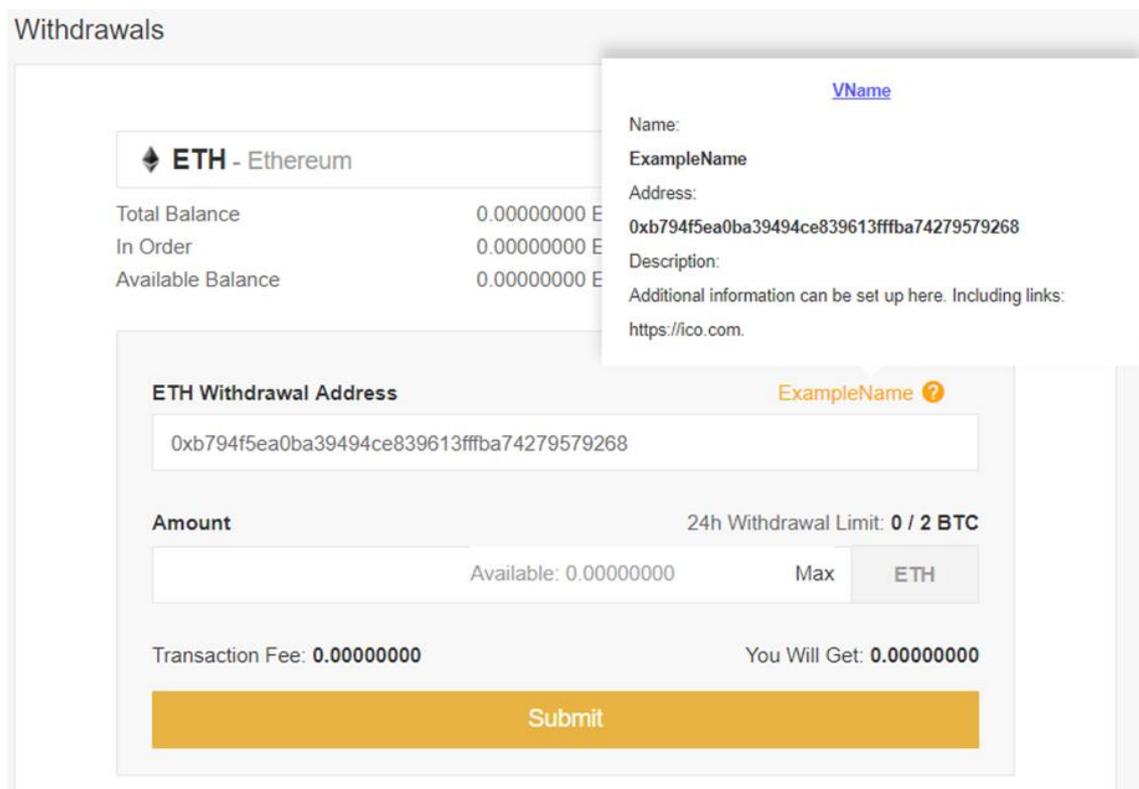
[15] This image is just an example. Any similarity to actual websites, exchanges, etc. are just a coincidence. We are not associated in any way or form.

When inputting the address, VName script will automatically detect the type of blockchain it belongs to and what is the matching nickname. Displaying this information plain text with an option to extend for more information.

This will work for every site that imports our JavaScript.

Browser extensions are in the works, which will remove the necessity of a particular site importing our vname.js and will automatically detect any address on sites visited and display the corresponding information.

Information will contain:

- Nickname for that address.

- If this nickname is verified or not

- The address itself.

- An optional description for this address

- Other information might be added in the near future.

3.4.   Demo

A demo of VName smart contract is deployed on Rinkeby, can be tested by accessing our site https://vname.id

It allows to find out the nickname of a specific address and to assign a nickname to the owner of certain account. Search can be used by anyone, however for assignation the user needs MetaMask browser extension.

In this demo, only Ethereum address are accepted.

Following picture is a demonstration of search functionality.
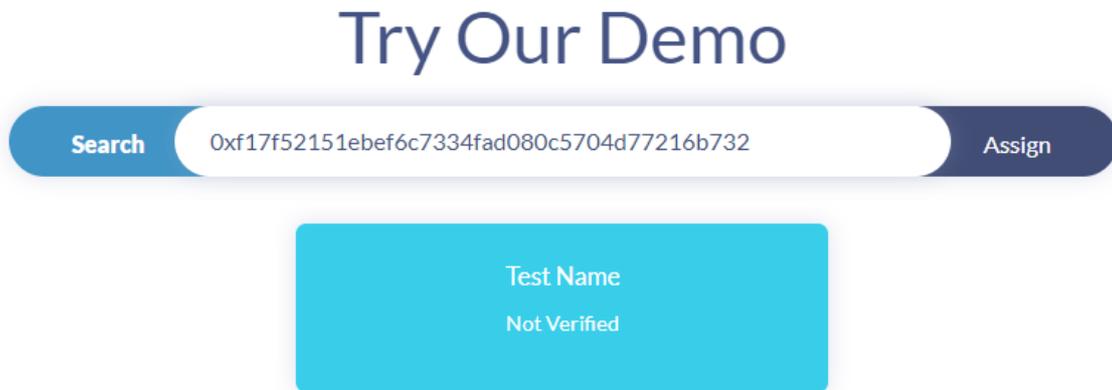
This picture shows how assignment works, clicking on assign will prompt MetaMask confirmation dialog.
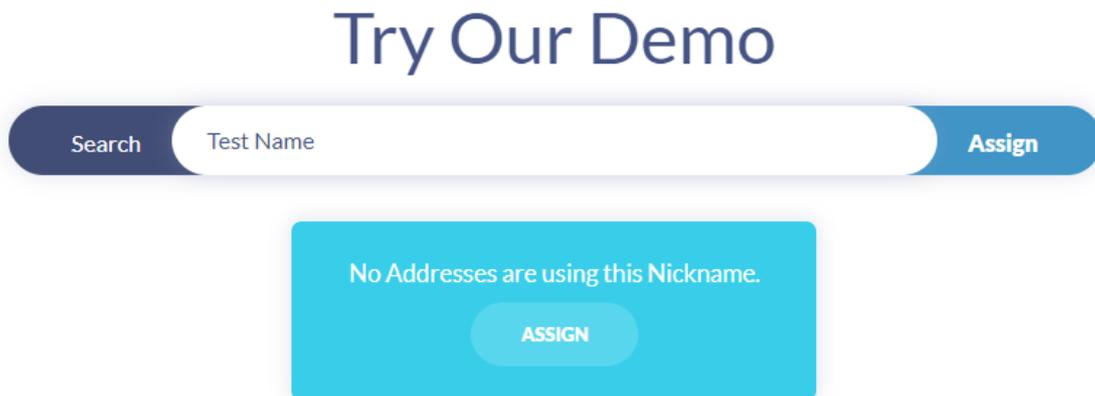
3.5.   Technology

VName works by storing a user's nickname, as well as what blockchain platform their address belongs to, and if the nickname is verified, in a mapping that is accessed by their address. It is built in a way so that you can only know the nickname of someone if you have their address, and not the other way around.

The closest reference to a nickname's associated address is a hash of the address stored with the nickname, which is solely used to verify the address on a nickname from outside of the mapping, and can in no way be reverted back to an address. This is intended so that VName can be used to verify that an address belongs to someone, but prevents being able to reverse-lookup an address by using a nickname.

VName allows anyone to associate a nickname consisting of alphanumeric characters to their address with a maximum limit of 32 characters.

2.2.1. Verification

There are two types of nicknames: verified and unverified. An unverified nickname is, and will always be, free to associate and has to be at least 6 characters long. These nicknames are completely open for anyone to use even if someone else is already using them.

Users of an unverified nickname can choose to verify it if it hasn't already been verified by someone else. This process involves paying with VName Tokens (NAME).

Verified nicknames have an advantage over unverified ones in that there can only be one verified nickname for every possible nickname.

Nicknames with a length between 1 to 5 characters are available only as purchasable, verified nicknames.

We provide the free, unverified option for users who want a nickname but aren't worried about others using that same nickname. For people who want an extra layer of authenticity, we provide the verification option so that no one else can have a verified version of that nickname. Unverified nicknames are displayed normally whereas verified ones are given either a verified symbol or a verified subtitle. This is ideal for extra security for ICOs, exchanges and similar businesses in order to avoid scams or other malicious intents.

2.2.2. NAME Token

NAME uses our own custom token protocol based off the ERC-20 and ERC-223 standard called COALITE[16]. This protocol allows the user to call the transfer function for NAME and send the adequate amount of tokens to the VName contract, which then accepts the sent tokens and verifies the nickname only if the right amount was sent.

In the event that an incorrect amount is sent, the VName contract will revert the transfer preventing the tokens from being taken out of the user's balance.

---

[16] COALITE was created as ERC-223 lacked some fundamentals methods for transfer and payment safety. COALITE is ERC-20 compatible.

4. VNAME Economics

4.1. Potential Market

VName is a system that will allow reducing transaction risk. From this perspective, where transactions will be made more secure under a decentralized system compatible with all blockchains, it is possible to speak of a potential market of 100% of the address holders of existing and future blockchains.

When considering the existing addresses of the blockchains of Ethereum and Bitcoin, they have shown exponential growth, accentuating it in recent months. As of February 2018, Bitcoin blockchain wallet users totaled 22,836,576[17], while the number of Ethereum addresses totaled 25,254,067[18]. This is a total of 48,090,643[19] potential users as of February 6, 2018. Assessing the trajectory, just three months before, the number of potential users amounted to 33,150,578 as of December 6, 2017. This implies an increase of 45.06%[20] in just three months[21] [22].

Taking into account the speed that has taken place in the growth of crypto users, the figures are an estimation since it is extremely complex to assess the growth of the market in the medium term. However, observing historical trends, it would not be surprising if the market doubled its number of users in a period of six months.

4.2. Financing

The financing mechanism selected will be in DAICO[23] format by issuing VName Tokens under the NAME code. Investors are informed that this financing mechanism will be the complement of

---

[17] Source: https://blockchain.info
[18] Source: https://etherscan.io
[19] It consists of the sum between the amount of bitcoin blockchain wallets and the number of Ethereum addresses.
[20] Which represents 14,940,065 new potential users.
[21] It is noted that, in the mentioned period, the beginnings in the regulations of China and South Korea took place, among others. As noted, this did not affect the upward trend in the number of users of the different blockchains.
[22] It is important to remember that these are the users of two blockchains. In other words, it is understood that the potential market mentioned is underestimated since it does not consider the total of blockchains and cryptocurrency.
[23] See section 4.3 for more information.

the one already used where 10% of NAME were acquired by private investors. The 10% was valued at USD 1,075,000 at the end of 2017.

The issuance of tokens will be of NAME 300,000,000 that will be divided:

(i)   10% was acquired by private investors[24].

(ii)   10% in incentives to generate strategic alliances with the blockchain wallets and exchanges[25].

(iii)   10% will remain in the hands of the founders of VNAME[26].

(iv)   5% will be used for bounty programs[27].

(v)   3% destined to advisors[28].

(vi)   62% destined to the DAICO[29].

Graph 3. NAME distribution
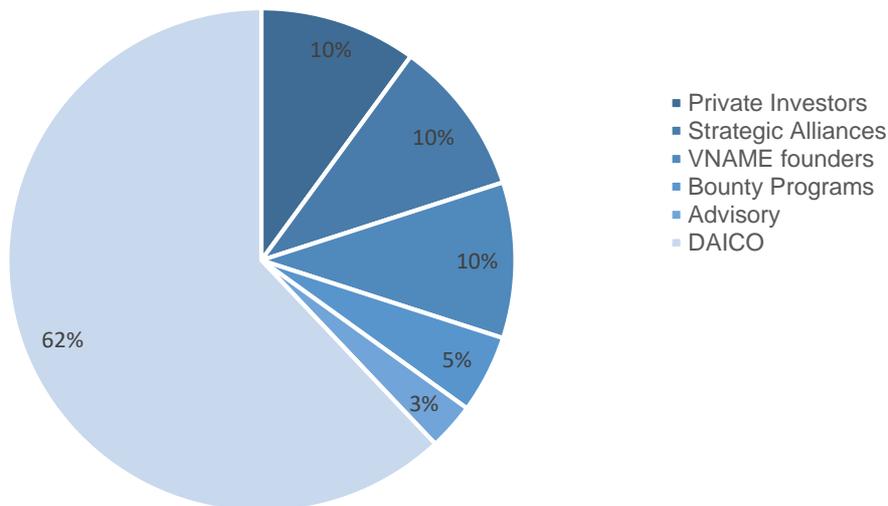
The investment round[30] will consist of five stages where a differentiated price structure will be used that will follow the following format:

---

[24] NAME 30.000.000.
[25] NAME 30.000.000.
[26] NAME 30.000.000.
[27] NAME 15.000.000
[28] NAME 9.000.000
[29] NAME 186.000.000.
[30] The level change will be automatic.

Table 4. Finance Structure by Stage

Stage	# Tokens	Share	1 ETH = NAME
Pre-Sale	14,880,000	8.00%	25,000
First level	24,180,000	13.00%	22,000
Second Level	37,200,000	20.00%	21,000
Third Level	50,220,000	27.00%	20,000
Fourth Level	59,520,000	32.00%	18,500
Total	186,000,000	100%	ETH ~9194

The difference between investing in the Pre-Sale stage with respect to level four will be ~35%. All NAMEs that have not been sold in the established funding period will be burned[31].

For the financing to be considered effective, a Soft Capital of NAME 60,000,000 must be achieved, reaching the equivalent as the total sale of the Pre-Sale and First Level stages, and the sale of ~55% of the Second Level. If the minimum level required is not reached, the purchases of NAME will be returned to the investors.

4.3.   Use of the Financing

When investing in VName, the investment made by the token holders will be used for business development. After identifying the main areas that will make up the business and estimating their budget, the token holders are informed that the use of their investment will be as shown in Table 5.

---

[31] That is, they will be destroyed. As an example, if in the DAICO´s NAME 186,000,000 were NAME 10,000,000 that have not been purchased, the total of NAME tokens after financing will be NAME 290,000,000 instead of the original NAME 300,000,000.

Table 5. Destination of the Financing[32]

Item	Description	% DAICO
Software Development	Integration	38%
	API development	
	Maintaining	
	Security	
Marketing	Positioning	24%
	Promotion	
	Communication	
	Presence	
Business Strategy	Cost Optimization	10%
	Development of New Business	
	Competition Analysis	
	Market Opportunities	
Strategic Alliances	Incentives	10%
	Contracts	
Team	Reward for a year of R+D	10%
Operating Costs	Equipment	8%
	Administrative	
	Translations	
	Legal	
	Consultancy	
Total		**100%**

As noted, the business was evaluated from a holistic perspective. The VNAME team considers that global success is associated to the different angles of the business, for which the budgets were evaluated independently.

In case of making the second issue described in the previous point, said financing will be divided among the items in a percentage manner.

---

[32] The elements included in the destination of the financing are in general terms. After beginning operations, the items could present small variations based on operational and business's needs.

4.4.   DAICO

It is a new financing model that contains the main benefits of its predecessors, the DAOs (Decentralized Autonomous Organizations) and the ICO (Initial Coin Offering). The model was proposed by the founder of Ethereum with the aim of obtaining a less risky financing for investors in a decentralized manner. The DAICO format allows token holders to control the withdrawal of funds, while also allowing to close the project in case the team fails in the development, realization or execution of this.

The DAICO consists of three primary phases: The **Announcement phase**, the **Investment phase**, and the **Development phase**.

4.4.1.   Announcement Phase

During the announcement phase the DAICO can't be interacted with and is merely present at this point so that potential investors have access to it for when it enters the investment phase.

4.4.2.   Investment Phase

During the investment phase, those who are interested in the VName project can contribute to the project and purchase NAME tokens similar to how an ICO works. All VName investors will be rewarded a free verified nickname with a minimum of 4 characters as a bonus for participating in the crowdsale. After the investment phase finalizes, the DAICO will enter the development phase, which is the important phase and the one where the DAICO comes into play.

4.4.3.   Development Phase

The invested funds are stored within the contract and cannot be withdrawn by any party. They aren't immediately taken from the DAICO but rather is slowly taken out from the contract at a defined rate (tap). The tap can be only incremented by polling.

4.4.4. Main DAICO features

The main points of the DAICO insured by the Intelligent Contract will be the following:

(i) Tap will initially be settled to 100,000 gwei / sec. Which is equal to 0.0001 eth / sec. This sets a weekly limit of withdrawal to around 60 eth / week. These withdrawals will be to guarantee the operation and improvement of VName[33].

(ii) In case an increase in the withdrawal limit is necessary, said increase will be submitted to a vote where all the NAME holders will participate. The system will be through a simple majority[34].

(iii) To create a withdrawal limit increase poll, at least 15 days since the last poll must elapse.

(iv) To reduce the risk of voting fraud, each token holder that has voted will get their tokens frozen 1 hour before to 1 hour after voting finishes.

(v) The date and duration of polls will be announced at least 48 hours in advance, otherwise, they cannot be created.

(vi) The withdrawal poll will be considered valid if a minimum of 20% of the holders of NAME participates[35].

(vii) The project closure poll will be considered valid if a minimum of 70% of the holders of NAME participates[36].

(viii) VName team is the only party able to create withdrawal limit polls. Any token holder is able to create a poll for dissolving the company. In this case of closure, the funds will be sent to the accounts of the token holders based on their participation[37].

---

[33] This does not imply that the withdrawals will be those, it only implies that if necessary to withdrawal that amount, it will be possible.

[34] IF (YesVotes > NoVotes; Yes; No).

[35] Exchanges cannot participate in the vote. The VNAME team will use the relevant algorithms to limit the participation of the exchanges.

[36] Exchanges cannot participate in the vote. The VNAME team will use the relevant algorithms to limit the participation of the exchanges.

[37] As an example, if an individual owns NAME 3,000,000 out of a total of NAME 300,000,000, 1% of the company's funds will correspond to it.

4.4.4.1.   Drafts and polls

Our DAICO smart contract uses a Poll Factory Smart Contract to create **Drafts** and **Polls**.

Drafts & Polls Functioning
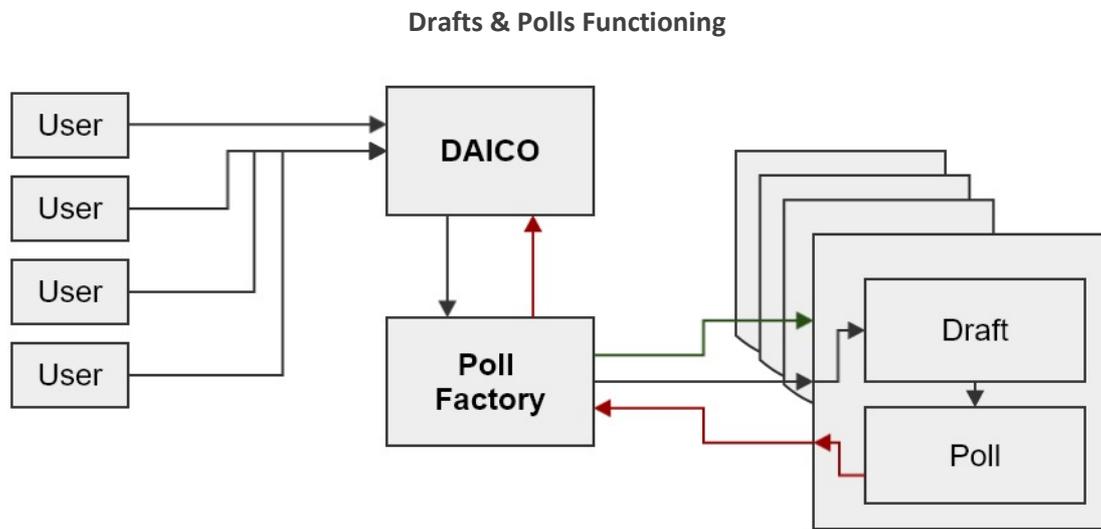
- To create a poll, first a draft is created where the poll is announced.[38]

- For a draft to be converted to a Poll, it needs a 5% of total supply votes.

- There must be a minimum of 48 hours for a draft to be converted to a Poll.

- Polls should be formatted so it depicts an action, being the only options YES or NO.

- Draft creation regarding project closure can only be initiated by holders of at least 0.1% of total supply.

- This Poll Factory might be used for many other different types of polls besides just withdrawal limit poll and project closure poll.

- All events communication will be transmitted via email to the registered holders, as well as displayed on VName official site. This events include:

  o   Drafts creation

  o   Poll creation

  o   Reminder to vote

  o   Draft/Poll close and results

---

[38] Polls can be created directly by VName.

- Votes are based off amount invested (# of NAME tokens hold) with a maximum vote capacity of 0.1% of total token supply.

- A vote can only represent a YES or NO (agree or disagree).

- Voting on polls is mandatory, failing to vote will decrease the holder voting power.

4.5. Business Plan

4.5.1. Business Strategy

The goal of the business strategy will be to generate as many benefits as possible to increase the value of VNAME in the market. With this objective, an agreed strategy was designed, which will have different stages.

(i) The use of the verification protocol for the safe conduct of transactions will be free for the first three months since the launch of the system. The objective of this is none other than to achieve universal VNAME usage and demonstrate its benefits.

(ii) 3 months after the launch of VNAME, there will be a charge for verification. The amount charged will be studied in conjunction with the blockchain wallets, exchanges, experts in the field, market behavior, and business possibilities. Given that it will be aimed at an income based on volume, each collection will be insignificant in absolute terms. Likewise, should the results of the analyzes suggest that the collection of an extremely small amount of verification puts the VNAME valuation at risk, this point will not be carried out and other business strategies will be evaluated.

(iii) While all user names greater than or equal to the six characters will be free, VName will reserve the user names of one, two, three, four and five characters, which will be auctioned in a period of six months. a year and a half after the market release. Likewise, regardless of the number of characters, VName will reserve the use of the name of countries, capitals, high-exposure persons and companies belonging to the S&P500 index, Fortune 100, such as five-character user names or less, they will be auctioned off in the period of six months to 2 years after launch. Bid currency on auctions will be NAME tokens.

(iv) One of the major projects that VNAME is developing is the creation of a secondary market for user names. This consists of the possibility of buying and selling user verified names without this implying any type of risk in questions of security, verification and anonymity. At the beginning of the secondary market of user names, VName might charge a fixed fee associated with the purchase and sale of user names.

The increase in valuation will be achieved through the generation of a profitable business model.

4.5.2. Roadmap

What we've done

- Identify a problem & work on the solution

- VName project validation

- Functional Demo on Ropsten Network

- Exchanges' listing agreements

- Worked on exchanges using VNAME API agreement

- DAICO, polls and voting research and whitepaper.

Day Zero - March 14, 2018

- Website launch

- BitcoinTalk post

- VName Whitepaper v1.0 upload

The future

- **Q2 2018**:

  o DAICO begins

  o Public API (JavaScript)

  o Voting polls and standard whitepaper

  o VNAME browser extension.

  o Exchange Listing

- **Q3 2018**:

  o Verified nicknames market

  o Integration with several wallets and exchanges

  o Implementation of addresses verification in different blockchains / cryptocurrencies

  o Integration with ENS for automatic purchase.

- **Q4 2018:**

  o Adding additional data to nick registration (color, bold, font, and more).

  o Regular work to add compatibility to more cryptocurrency blockchains.

  o Migration of VName to its own blockchain network.

Appendix 1 - Ideas for DAICO

Disclaimer 1

This appendix was initially written as part of VName Whitepaper. However, due to the unexpected extensive research and analysis done, it was separated into this appendix and is planned to be release in its own whitepaper.

Disclaimer 2

This document is meant as a source of reference for concepts that could be applied to a Decentralized Autonomous Initial Coin Offering (DAICO) and are merely theoretical. The content within this document is in no way the standard on how to implement a DAICO and is instead a personal view on potential ways to build one. That said, the concepts explained here can be used should you choose to.

What is a DAICO?

A DAICO is at its core an Initial Coin Offer (ICO) but improved upon with features present in a Decentralized Autonomous Organization (DAO). ICOs have the problem where after the crowdsale phase ends the developers have access to all the contributed funds and may decide to keep the funds but not finish their project, effectively running away with all the money. Vitalik Buterin[39] suggested changes to the ICO format to provide investors with more control over their contributions. This would make it so that the developers won't have access to the crowdsale funds at first, but if the investors see that the developers are making progress on their project, they can vote to increase the rate at which the developers can claim funds, but should they see that the developers aren't complying to what they promised, the investors can vote to close the DAICO and reclaim any remaining contributions.

Objective

The objective this document will try to work towards is to establish an ideal DAICO where neither the developers nor the investors are at a disadvantage. This will ensure that the investors are

---

[39] Russian-Canadian programmer and writer primarily known as a co-founder of Ethereum and as a co-founder of Bitcoin Magazine.

given control over their funds, but will then be responsible of participating in polls related to the DAICO.

An Investor's Power

What makes a DAICO is allowing the investors to control the money they contributed to the project. Since it's their money, they should have some ownership of it and be free to take back the remaining money they have if at any point they aren't satisfied with the project. It is recommended though that investors make decisions as a group as opposed to individualism, as this will ensure that actions are agreed upon by the majority instead of any single person deciding to remove their money and affecting everyone else due to the change in funding. In general, the recommended format for a DAICO is a democracy.

With Power comes Responsibility

The difference between a DAICO and an ICO is that, before, the developers would be solely responsible of all the contributed funds, whereas now, the investors are responsible. Before, when there was a risk of developers misusing the money they were given, now there is a risk of investors misusing the facilities they are given in this new format. Regulatory mechanisms should be put in place to ensure that investors stick to logical and justifiable actions and don't abuse the power they are given. It's important to remember throughout this document and, should you choose to, henceforth that investors are knowingly contributing to a DAICO and as such have a responsibility they are expected to oblige to.

Stakeholder's Democracy

In a democracy everyone has the same presence in an election, and this is made possible thanks to a legal identity and citizenship. In a blockchain environment though, one can create as many identities as they want, so all someone would need to do is create enough addresses to have a majority over the number of legitimate addresses and they would then have control over polls. To prevent this, not only should polls be made only available to investors of the project, but votes should be proportionate to the amount invested - albeit to a certain limit - so that even if a person decides to build several addresses, they'd still have to invest more than half of the total contributions in order to have control over polls, and given that they'd own more than 50% of the total funding at that point, they would theoretically own most of the project and as such have final word over what happens with the project. This form of democracy also has the benefit

of ensuring that a big investor isn't affected by several smaller investors simply because of the number of people, but instead if the total sum of the smaller investors is greater than the amount contributed by the big investor, at which point the smaller investors have majority over the project.

The Problem with DAICO Voting

Contributors can choose not to vote; affecting the amount of people that vote, and in most cases, affecting the outcome of a poll.

Potential Solution

Publicly announce ahead of time that a poll will be held and penalize those who do not participate in polls.

The main issue in the way that a DAICO is built upon is that it heavily depends on the constant participation of the contributors and any negligent behavior on their part heavily affects the project. To ensure this doesn't happen voting must be enforced to some degree so that contributors are obligated to do their role. This can be solved either by providing incentives to vote or by providing penalties in the event a contributor does not vote. Due to the nature of a DAICO and the role contributors take when investing in one, the incentive route would affect the way contributors view their votes - from being their responsibility to merely being a way to gain something extra - and for this reason the penalty route is recommended.

The idea behind placing penalties on people who do not participate in elections isn't a new concept, and its proven effective in most occasions where it's used. It's important to remember that the objective here is to educate contributors of their responsibilities when investing in a DAICO.

Potential Investors should be told of the policies regarding polls before they invest in a DAICO. It should be designed so that everyone who invested was because they agreed to the responsibilities set upon them. This is also essential to validate the penalties being put in effect as something that was agreed upon by ALL contributors and not a DAICO's abusive nature. There are different ways to handle negligent contributors, but they mostly share similar concepts in that people who don't vote are valued less over people that vote.

Decrease in a Contributor's Value in a Poll

The idea here is that at first polls function like any regular election: "1 person, 1 vote" ***** , but in the event that someone doesn't vote their election value drops, so instead of being valued at 1 vote, their vote is valued at 0.9, 0.8, etc. This method ensures that people who don't vote are gradually phased out of the pool of voters, so that their blank vote doesn't affect the absolute outcome of an election. For this it's recommended that polls be designed in a "vote for an action" fashion, so that those who don't vote are in the same group as those who voted against the action (because of how people manage action and inaction, people are more likely to contribute if they agree to something than if they disagree)

Organize Polls by Tier

A tiering system could be used to regulate who gets to vote for what and at what level must their presence within the DAICO be in order to vote for a certain tier. This idea is meant to allow everyone to vote for simpler things, while require some level of presence for some more serious things. The mechanic which determines what tier a contributor has access to can be built around different variables, for example: what percentage of the total investment does a contributor own, how active are they in voting, or how trustworthy their word is in a poll. This doesn't necessarily have to be restrictions on who gets to vote for what, but rather who gets to initiate a poll; the tier requirement for a poll can be different for the initiation and the election. The reasoning behind this is to prevent people who invested a miniscule amount in comparison to everyone else from initiating a poll to disband the DAICO. A better implementation is one where a sort of community can exist between contributors in which they can discuss if a disband poll should be created and then those who had invested a greater amount in the project (that on average would be people who are more adept at investing and they saw potential in the project) can initiate the disband poll for everyone to participate in.

Drastic Measures - Removal of ability to vote and ownership of investments

This is merely a hypothetical suggestion and should not be used unless the state at which investors function becomes extremely negligent and uneducated. These concepts aren't fully recommended because of how they break the nature of a DAICO but depending on the circumstances this drastic behavior might be the only way to transition people from an ICO format to a DAICO one. The idea behind these concepts is self-explanatory: penalize negligent behavior by removing a contributor's ability to vote in polls and in extreme situations remove

their ownership of the funds they invested (both of these things can be either for a period of time or permanent, and in the case of their investments can be either partial or absolute). This doesn't *fully* destroy the DAO functionalities in the DAICO but it heavily restricts them.

Drafting a Poll

In some scenarios, it might be better if there was a consideration phase before issuing a poll. For this a draft could be implemented. A draft is at its roots a poll, but it doesn't carry the same requirements or impact an actual poll has. In this format, anyone can initialize a draft, even if the poll this draft is based on has a minimum initializing tier. What a draft allows is for investors to see who's interested in a particular poll before initializing the poll. Drafts can also serve to ensure that the big investors agree with having a poll before it is actually created. Drafts are also optional, so investors are not required to participate in them and they won't be penalized if they decide not to. To ensure that people have a chance to know about the poll before it's initialized, the poll should only become active after a minimum of 48 hours since the draft was created.