# The CRWD Network

Daniel Horak, Paul Pöltner

July 16, 2018

**Abstract**

The CRWD Network is launched by CONDA Crowdinvesting to establish a standardized protocol to offer regulated financial products on top of an open blockchain. Through KYC verification, wallet addresses can be linked to a customer's real world identity, allowing for new, legal ways of asset type fundraising directly on the blockchain. The newly established decentralized network of crowdinvesting platforms achieves this without handling any fiat currency, which makes it easy to scale across countries and jurisdictions.

## 1 Introduction

Crowdinvesting has increased in popularity in recent years, as access to capital has shifted away from traditional financial institutions towards a more decentralized type of funding. This has various beneficial effects in that the risk-averse nature of traditional institutions often fails to fund ideas that are high in risk because analyzing and financing them does not pay off for bigger institutions. Also, the timeframe in which monetary funds can be acquired can potentially be decreased for projects, making it possible for them to get off the ground quicker and with more fitting funding than bootstrapping methods. Underserved projects of this kind can be found in various areas, from small medium size enterprise ideas to big real estate ventures.

While the whole area of alternative financing has seen significant growth in Europe [1], the proliferation of another type of less regulated fundraising has been felt heavily in the global financial industry. This type of fundraising in the form of initial coin offerings has been exploding in a short time frame, leading to massive amounts of money being raised. That is because many of those fundraising methods are comparatively frictionless and fast, operating in legal grey zones while being marketed to a global audience of buyers. The legal grounds on which they operate are shaky at best. Because many concepts shaping the future of decentralized markets are being influenced by those mechanisms, we must pay close attention to these events.

This paper is here to describe a network concept that combines both worlds, that of regulated alternative financing and that of blockchains supporting lightly regulated smart contracts to build a crowdinvesting platform utilizing the technological advancements of decentralized technologies.

# 2 Ideas & Background

The CRWD Network builds on various innovations that have been developed since the release of the first blockchain. Here a short overview of the background and decision-making in founding the project.

## 2.1 Problems Solved by the CRWD Network

The network tackles the problem of how KYC can be brought to the blockchain across multiple jurisdictions. Furthermore, it allows the crowdinvesting concept to spread across multiple countries without having to deal with the legal hurdles of handling multiple fiat currencies.

If done right, blockchains and smart contracts can automate a lot of processes and create clear structures for various stakeholders in the network, incentivizing them to work together to achieve common growth. In addition, the CRWD Network can be further and further decentralized to leave more functions to the CRWD community itself rather than to formerly-centralized entities.

## 2.2 Choices in the Decentralized Smart Contract Environment

When choosing a blockchain on which to build the network, there were various points to consider. Firstly, building a separate blockchain for this kind of purpose is ill-advised. Lots of different networks like Ethereum, Ethereum classic, Neo, NEM, Tezos, EOS are either in long-term development or are constantly changing, incentivized through complex proof-of-work or proof-of-stake algorithms that will ultimately make them a more secure solution to use for the task at hand.

The CRWD Network should be built on a decentralized, public blockchain that would still run for some time even if the leadership team changes, quits or stops developing in order to give sufficient time to change to another blockchain technology should it be necessary.

Also, blockchain technology in general is rather new, and many of the projects, while promising, either have not yet launched or have not been sufficiently tested for any type of big scale implementation. Other blockchains like bitcoin don't support smart contract and tokens natively, and while solutions like RSK for the bitcoin blockchain are being developed, they are not ready for production.

As the aim is to build the initial network on a proven blockchain system to be as safe as possible with investors' funds, the CRWD Network utilizes the Ethereum blockchain, which has already more than 66160 ERC20 token contract deployed. [2] Its Solidity smart contract language is also the most proven at the moment. Alternatives exist (e.g. Flint) [5], but they have not been tested to the same extent as Solidity. All technologies considered are currently lacking in decentralization, scalability, community trust or some combination thereof. As trust and decentralization are the most important factors for the project, Ethereum is a good choice. Altough some scalability issues [6] have yet to be addressed in order to stay on the blockchain for a long time, some improvements are in the making like Sharding [7] [8], Raiden [9] and Plasma [10] / Plasma Cash [11]. They will obviously be closely monitored.

Ethereum Classic (ETC) is the alternative fork to Ethereum (ETH) and could also serve as a fallback option in the event the now more popular chain fails.

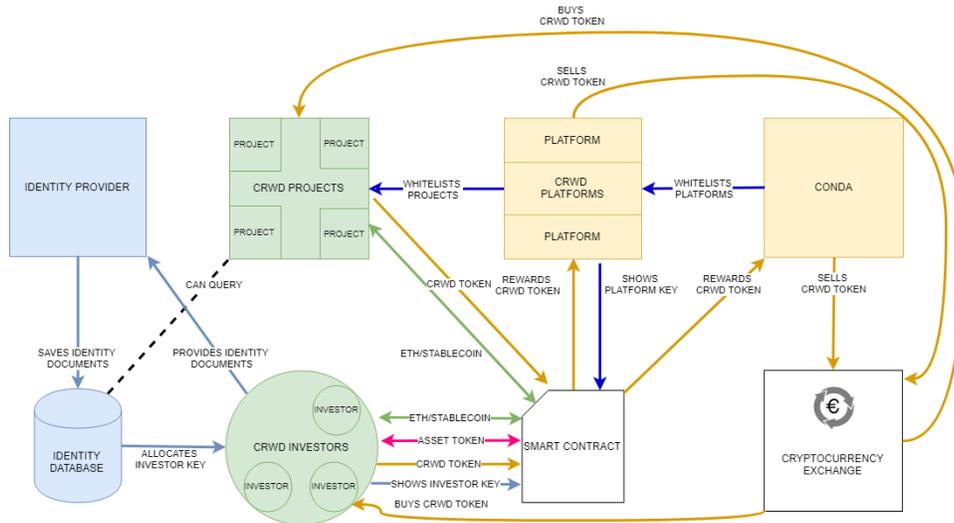# 3   An Overview of the CRWD Network



Figure 1: An Overview of the CRWD Network

The CRWD Network has various areas and will build upon a row of smart contracts. The upcoming section explains parts of the network in subgroups to make it clear to technically-inclined readers how the network will be constructed.

1. Token Types and Involved Stakeholders
2. KYC Process and Investor Keys
3. Platform Verfication and Platform Keys
4. CRWD Asset Project Release, Fundraising and Finalization

## 3.1   Token Types and Involved Stakeholders

The CRWDToken Ecosystem has two types of assets and two types of verification tokens utilized to facilitate the platform's functionality.

- **CRWDToken** - The CRWDToken is the inherent utility token of the CRWD Network. It is an ERC20 standard token that is utilized by various services in the network and has fluctuating value based on market trading price.

- **Asset Token** - Once a company has launched its fundraising on the CRWD Network, it issues a tokenized equity offering also commonly referred to as asset token. This token represents the company's liability to its investors and can come in the form of any financial instrument like a share or a bond. It is generated automatically for each new project on the network and can be traded and held within identified Ethereum wallets.

4

- **Investor Key** - An investor key is an unmovable token issued by the smart contract after the KYC process is finalized. It marks the owner of an Ethereum address as part of the CRWD Network. Through the key the person can be identified by a partner of the CRWD Network. An investor key allows an address to invest in CRWD assets.

- **Platform Key** - A platform key is issued to CRWD platforms and allows them to add new projects to the CRWD Network. A key of this kind is given out by CONDA after setup of a legal contract with the CRWD platform.

There are various entities that will be involved in the CRWD Network:

- **CRWD Projects** - Entities that launch an asset token representing their shares or bonds on the CRWD network.

- **CRWD Platforms** - They are the local entities that decide to verify and list projects on the network. Anybody can apply to become a platform provider to add projects into the CRWD Network by getting in contact with CONDA and agreeing to a joint policy on how to deal with new companies.

- **CRWD Investors** - Investors want to use the CRWD Network to buy regulated asset tokens of a project they likes. They subsequently go through the KYC process, get an investor key and start to spend Ether and Stablecoins on projects they like.

- **CONDA** - CONDA whitelists platforms by giving out platform keys to partner platforms. In addition, it is responsible for the further development of the smart contract environment and the adaptation of the network to the community's needs.

- **Identity Provider** - This can be a third party that checks the KYC status of an investor and, after successful verification, triggers the Investor Key handout. They save the KYC data of investors and give projects access to it when necessary.

- **Cryptocurrency Exchange** - A cryptocurrency exchange is an independent entity for the trading of cryptocurrencies. It can be decentralized in the form of a smart contract or have a centralized (usually higher capacity) bank-style platform. Furthermore, many exchanges are not yet willing to trade asset tokens, which is why most tokens currently traded are utility tokens. CONDA expects security tokens and their exchanges to play a bigger role in the future and are therefore in talks with security token exchanges like Gibraltar Blockchain Exchange [12] and Finhaven [13].

CONDA will focus on listing the CRWDToken on various utility token crypto exchanges. For asset tokens CONDA is already in negotiations with exchanges that support special token types to help projects with getting listed. Because many exchanges have their own individual guidelines, projects are ultimately responsible for their own listings; however, CONDA will offer support as possible.
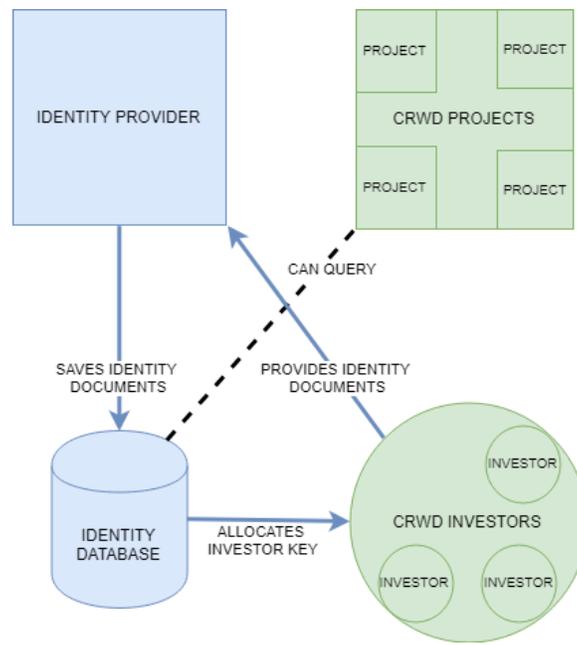
## 3.2 KYC Process and Investor Keys



Figure 2: KYC Process

The CRWD Network allocates regulated assets and shares to participants while ensuring that a standardized KYC process is followed. This section briefly explains the initial setup and verification a new user has to go through to participate in the CRWD Network.

The investor key serves as the central point of contact between identity data and its storage location and is verified on the Ethereum blockchain. With this key, an investor can verify his or her identity across multiple projects while only having to go through the verification process once; it even ties one's identity to multiple KYC-compliant and verified Ethereum wallet addresses.
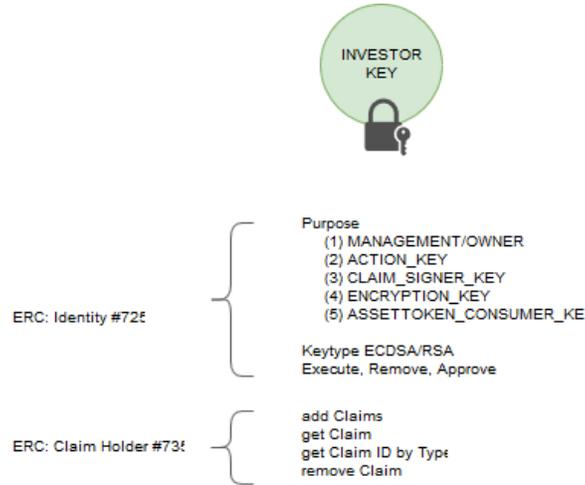
### 3.2.1 The Investor Key Smart Contract



Figure 3: KYC Process

The CRWD Network investor key is modeled after two proposals for identity standards, the EIP 725 [3] and EIP 735 [4], both of which were proposed and developed by Fabian Vogelsteller, who also introduced the ERC20 token standard. These identity standards work together to create an identity format for the Ethereum blockchain that can be used to flexibly verify and add identity verifications.

For the implementation, both standards are used in conjunction with each other and are published into the same smart contract. We'll shortly review the workings of the EIP 725 and 735 standards and then go into details on what has to be adapted for it to be usable for our asset token crowdfunding case.

### 3.2.2 EIP 725 Identity

This serves as a contract that saves an identity on the blockchain and executes functions that handle key management. The contract can handle various levels of keys starting from the Management Key (1) to Action (2), Claim (3) and Encryption (4) key. These keys have a decreasing level of control on the functions in the smart contract, with the management key having the highest "access control".

The management keys (1) represent the wallets which will be allowed to hold and send securities tokens. It can also add any additional keys that are allowed to interact with the investor key. Action keys (2) can be used as a safer alternative to handle approvals of claims. Claim keys (3) are revocable

7

and are given to third parties that are allowed to make claims in the contract. Encryption keys (4) may include encryption information for the claims that have not yet been accepted. The Asset token consumer key (5) is added for the purpose of the CRWD network and is not part of the EIP 725 standard. The key type is saved as an extra variable with the keys and notes if a given wallet uses RSA or ECDSA encryption.

The process for using this part of the smart contract is that a person first generates an investor key for an address, which is a new contract on the Ethereum chain. The contract can then be triggered to add claims by third parties and claim holders through EIP 735.

### 3.2.3 EIP 735 Claim Holder

Any information a claim holder has about an investor key owner (represented by the management key) can be added through EIP 735. The claim holder can, for example, verify passport data and ask the identity key owner to add the approved data to his/her investor key via an "addClaim" command. The manager of the investor key then has to approve that this new claim from a third party can be added to his key. A claim holder will most likely add their claim to a predefined "type" of standardized claims that can be added to the investor key.

The type of data that can be saved through these claims is various and will include what type of data is saved, how that data can be verified, who made the claim, the signature of the claim provider, the hash of the data and the url of where the data is located.

Typical claim makers are 3rd party ID service providers that receive the ID data and verify their authenticity. Upon acceptance of the document's validity, these providers certify that they have checked the claims and found them to be legally-compliant. A claim of this kind comes in various levels and is based on what stage of compliance is needed, in the case of most European countries, this could be:

1. Passport verification - until 5000,- Euro equivalent investment
2. Video identification - from 5000,- Euro investment upwards
3. Proof-of-fund origins - above 100.000,- Euro

An owner has the opportunity to reject a claim without need for clarification, and he/she might do that in cases where the information submitted is incorrect or no longer factual. He/She can also chose to ignore wrong claims all together and never verify them if they shouldn't be included in the investor key.

This contract can be queried easily through the "getClaim" and "getClaimID-byType" command so that existing claims can be easily accessed.

### 3.2.4 Differences in the EIP 725/735 Standard for the CRWD Network

While the CRWD Network is modeling the investor key after those two standards, some changes have to be adapted so that it can work for the task required.

* Asset Token Consumer Key

An additional key type was included which can list the projects that have current access to the ID records of the individual. This has to be added for legal compliance reasons, as legal requirements in some jurisdictions require that projects themselves need to be able to check the validity of the KYC'd data directly.

* Data Storage Differences

The standard recommends decentralized file storage networks like Swarm or IPFS, but these are still in their early stages of development. That is why it is necessary to save the original ID data with a service provider for now. This provider can also handle sending claims to investor keys so that once a valid ID claim asks for verification, the ID operator will be able to send the new verified data directly to the investor key.

Furthermore, the storage provider should ideally be able to check when valid claims are added from somebody with access permission to the data to automatically grant them access to the data in their file system.

* Time-based Document Access and Revocability

Revocability of approval as foreseen in the standard has to be partly limited for legal reasons. According to the standard, once permission is granted, the identity holder has the right to withdraw this permission at any time. This is why we have two additional rules for revocation of ID access rights.

The contract will grant a project a new minimum time-based access where the projects have time to use the ID documents and check their validity themselves or, in case it is legally required, save them on their own servers. The decision was made to add this timed access to forgo a problem where somebody grants access to the data just for a very short period of time. In that case access will be granted on a timed basis likely a few weeks or months, which should give the project enough time to check for all legally required points.

The second requirement change is that revocation of access rights can only happen once the investor key is emptied of all assets that need permanent record access. During revoking of the access rights a check will happen to see if any asset tokens are left on the key that need those rights. If this check returns

false, the investor key holder is reminded to first move the tokens to another wallet verified by an identity key (e.g. sell them) to be able to revoke the ID access rights.

To stay GDPR-compliant in the EU, projects will have to agree to delete the data not needed any more, and the data storage provider will have to do the same. While the hash values of the ID documents will stay on the blockchain, the saved files they link to can be deleted to stay within the new laws.

* Simplified Claim Addition

To simplify the user experience, we are opting to create a whitelist for service providers that are allowed to add finished ID verification claims directly. The user will not have to go the extra step by approving the added claim from a pre-approved provider. This helps the CRWD Network to be one transaction faster, while still allowing third parties to add claims if the investor key holder wishes to do so.

### 3.2.5 Interaction from the Investor Key with the Clearing Contract

The clearing contract for the CRWD Network checks if the legal requirements are met by querying the information saved in the investor key. It is used to transfer the asset/security tokens to another investor key and collects a small fee in CRWD tokens for that service. This fee certifies that legal requirements for the transactions have been passed, and CONDA is responsible to build up a network of identity providers which follow the same rules and policies. The clearing contract has a list of accepted identity provider wallets which can issue KYC claims (e.g. video identification) verification for the CRWD Network. The investor key owner that wants to receive asset tokens has to have a valid claim by an identity provider on the list in the clearing contract.

To guarantee that projects that need data access more frequently also pay for the service costs of the data storage, CRWD tokens will be subtracted from the project's wallet when ID documents of the verified investor keys holders are accessed.

### 3.2.6 User Perspective

From the user's perspective, the initial registration will require CRWDToken to trigger the KYC process for an address. The person has to prepare an Ethereum wallet with an investor key under his/her control that he/she wants to associate through the KYC process with his/her persona. For people holding lots of Ether, we recommend associating a newly-generated, previously unused address and sending it CRWDToken as well as Ethereum to facilitate the process in a more private fashion. It is possible for promotional reasons that the initial setup will be cheaper or not require CRWDToken in order to obtain the critical mass

of users needed to sign up during the network's launch.

Once the KYC process is triggered, the user will go through a standard process of proving one's identity. This can include up to three steps:

1. Verification with passport and facial photograph
2. Verification with live video
3. Proof of fund origins

A standard criteria for the KYC process has to be met in each jurisdiction. The KYC provider can be chosen by the local CRWD platform, though CONDA will help new platforms to choose fitting partners if there is a necessity for this.

This verification information is then saved in a centralized database. A decentralized version would be preferable, but due to security risks with operating such a platform in a decentralized manner, more research has to be done to shift all data to a decentralized data storage service and retrieval mechanism in the future. So far the investor key will save a verification and URL leading allowed parties to the documents.

The Investor Key address provided will receive a uniquely-generated, claim from the KYC provider that has a validity of up to three years, allowing for automatic future verification of a user's profile. This verified Investor Key will establish that the wallet is allowed to use CRWD services.

### 3.2.7   Individual Project Perspective

The investor key linking KYC documented identities with real addresses on the Ethereum blockchain benefits projects by lifting the barriers to entry on the CRWD Network. They can save on KYC costs by spreading the costs of the KYC process across many people around the world. Beforehand, new projects needed to perform a new KYC process with each of their respective investors. Now new projects don't need to identify each investor; rather, they can be sure that only individuals that have gone through the necessary level of KYC via their Investor Key can fund their crowdinvesting projects. In most jurisdictions, you must be able to identify all investors for legal purposes. By performing a query in an identity database, projects can now easily pull up the profiles of their investors as proof to local governments that regulations have been followed.

Furthermore also projects will have to go through KYC verification and work within the local prospectus and disclosure laws before launching their equity or debt based token. They go through this project with their local platform, which then also determines which investors from which jurisdictions are legally allowed to invest into the new project. The Investor Key automatically checks if the individual investor is allowed to invest into the new project. Therefore it will

also show which further verification steps are missing in case investment is not possible at this point in time.

### 3.2.8 Querying a KYC verified Profile

When a project needs an investor's data, it will be able to query the necessary information via the investor keys, to gain access to the database location where the files are saved. To discourage mass querying of investor data and to minimize overutilization of this service, investor queries will cost the project founders CRWDToken, thereby limiting such searches only to times when they are legally necessary.

The user must agree to be able to be grant the project KYC data access, before he/she invests or receives tokens from a project. Individual users will be able to refuse token transfers that they don't want to receive if they feel their data might be at risk with the project in question. This might be important in the case of airdrop campaigns that intend to reach a larger audience.

### 3.2.9 Exceptional Key Reissuance

In the exceptional case that access to private keys and the adjunct asset tokens are lost, a special condition in the smart contract will be triggered to reconfirm the investor through KYC to lock old tokens and reissue new ones. The complex nature of this process will incur costs that must be paid by the investor. To prevent this activity from security breaches, it is essential to go through a high level of the KYC verification in the reissuance process to make sure that stolen credentials can not lead to account theft.
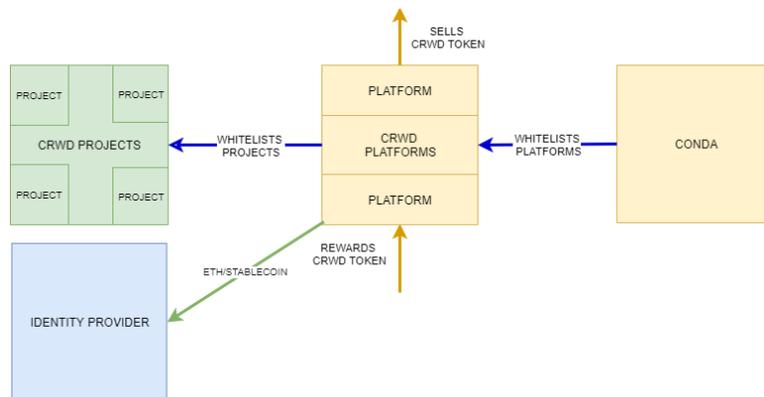
## 3.3 Platform Verification and Platform Keys



Figure 4: Platform Key Allocation

The platform keys are used to accept new projects to the network and issue security tokens. These keys are accredited and given out by CONDA and are then whitelisted in the smart contract.

The verification process of a new platform follows the same standards as previously performed by CONDA by setting up legal agreements with each platform to ensure quality. The platform can then whitelist projects via its own platform key. It has the option to use a CONDA whitelabel solution[14], which can quickly bootstrap its efforts to join the CRWD ecosystem with little hassle, so it can get started quickly to whitelist new projects on the network.

For each whitelisted project that raises funds in the CRWD ecosystem, the responsible listing platform will be allocated a percentage of the fees paid in CRWDToken. The platform also interacts with the investor whitelisting process, as it is responsible for adding investors to the network that can then internationally invest in all projects. The local platform therefore pays a chosen KYC provider to take care of the legally required process and allocate new investor keys.

When users invest in CRWD projects or resell their shares (by paying CRWDToken as fees), the original whitelisting platform will receive a percentage of these fees in order to recuperate the upfront costs of whitelisting investors and incentivize them to bring on investors that are actually willing to invest. It would be possible to have CONDA or a fixed partner take over the KYC process, but then platforms would be encouraged financially to list anybody, including those whom are not interested in investing. Letting the platform pay the fees makes it more likely that it will only target individuals for whitelisting that are interested in participating in the CRWD ecosystem. It might be possible in the future for people to chose their own KYC provider from a list and whitelist themselves in the ecosystem, but that would be part of the additional development of the network to streamline the growth process and further decentralize the choices people can make within the network.

## 3.4  CRWD Asset Project Release, Fundraising and Finalization

A project that wants to fund its efforts via the CRWD Network will get in contact with a local CRWD platform, buy CRWD token and set up its marketing campaign. In some cases, the local platform might support them in both steps.

### 3.4.1  Fundraising for a new Project

A fundraising process via the CRWD ecosystem has up to a maximum of 7 steps.
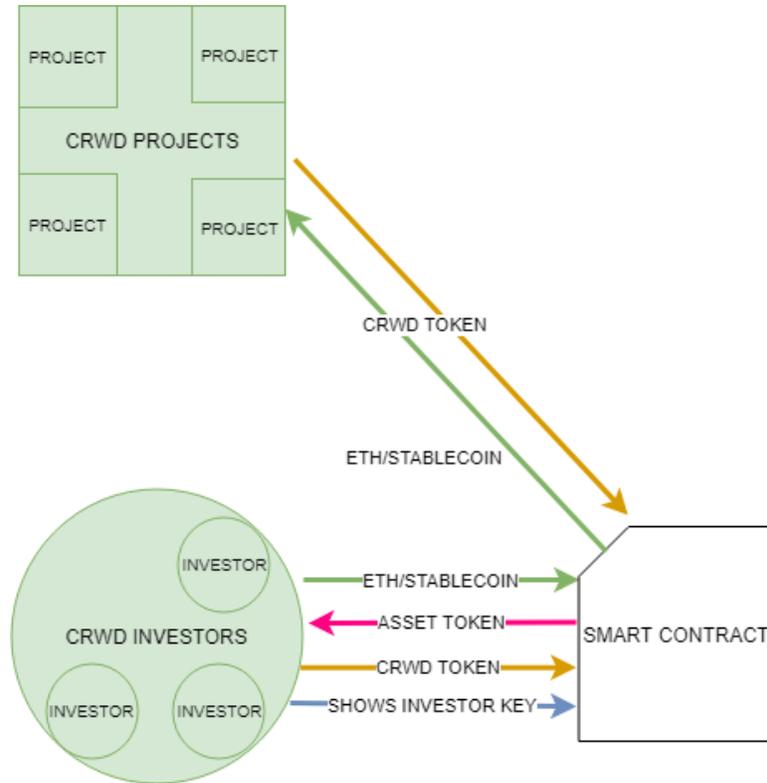
Figure 5: Asset Project Fundraising

1. The local platform helps the project set up all necessities for getting funding via the CRWD ecosystem and does a check if the local legal requirements are met by the project owner.

2. The CRWD project that needs funding has an active Ethereum address with enough CRWDToken to trigger the token creation process. At this stage, CRWDToken issuance companies need to think about how many tokens they want to generate, at what price they want to sell tokens and with which limits they want to set the standards for the upcoming funding process. These variables are permanent once the pre-sale process starts. The contract creation process is now triggered, and the project can be marketed until the official funding process starts. Alternatively, the project can start fundraising right away if everything necessary is in place and it has enough CRWDToken available.

3. The platform that chooses to whitelist a project triggers the whitelisting process via its platform key. The project will then be visible on the local platform and marketable to investors with a legally compliant Investor Key.

4. Investors can now use their addresses that are associated with their investor keys to send funds and fees (paid in CRWDToken) to the CRWD projects in which they want to invest.

5. By the end of the crowdinvestment deadline, the project has either reached its fundraising goal or pays back all tokens.

6. The company has the right to automatically refuse specific investors. All accepted investment offers incur a CRWD fee by the project that is raising the funding.

7. The smart contract will automatically allocate and forward fees paid to the whitelisting platform and other recipients.

### 3.4.2 Secondary Market

One reason for utilizing a blockchain infrastructure in the first place is the possibility to resell asset tokens before the end of the project to other market participants without having to go through a third party. Once corwdinvesting is completed, successful investors can resell their shares to other whitelisted CRWD Network investors on participating asset exchanges or in OTC direct agreements with CONDA as the escrow provider. They can also broker a deal without escrow if they know and trust each other by directly sending their tokens and payment to the other party. Each transaction of an asset will incur a small fee in CRWDToken and of course, in Ethereum gas. CONDA will try to entice professional market makers to also join in trading in the market, so that projects with less frequent trades can still be sold or bought under the year even if this comes at a slight premium.

The possibility of having a secondary market facilitates a better valuation of the project after fundraising is over and gives a glimpse into how the market values the project if it does better or worse than expected. Furthermore, an investor who wants to recoup all or part of his/her investment early can now do so easily by reselling his/her asset token at the current market price. CONDA is actively researching available asset trading exchanges that can facilitate the secondary market with higher velocity infrastructure.

### 3.4.3 Shareholder Voting

In some cases, asset tokens will be issued that actually represent shares in a company and guarantee voting rights. There will be a voting mechanism in the individual smart contract similar to shareholder voting outside of the blockchain, but the counting of votes and verification can be done automatically
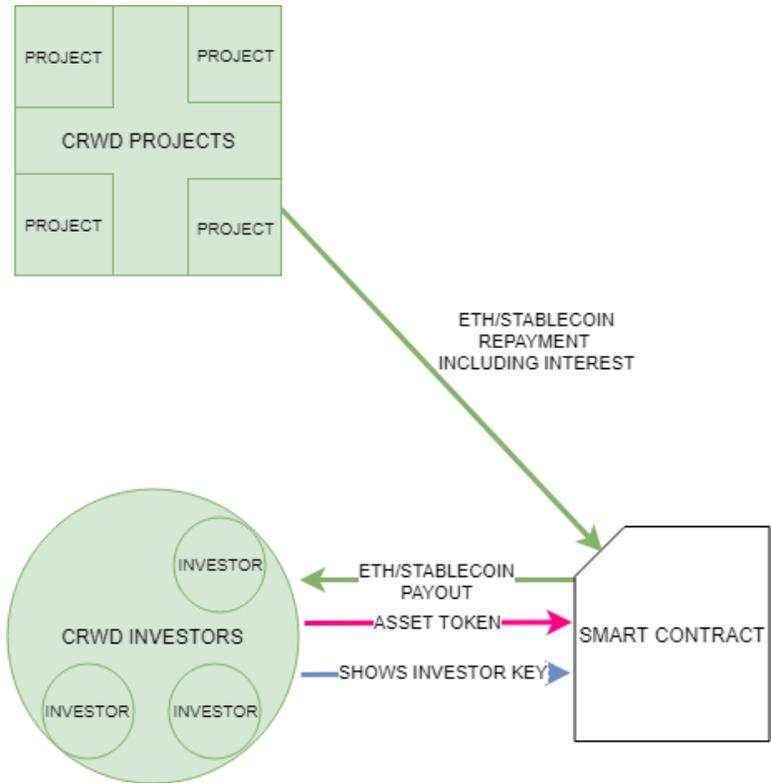
Figure 6: Asset Project Payout

and remotely by signing the adjunct investor key. Asset tokens that represent other forms of investments like preferred shares or debt bonds will not have voting rights.

### 3.4.4 Finalization and Payout of a Project

In case a debt investment was made and the investment period ends, the project will undergo a repayment process to send back funds and interest to investors. This process resembles a repurchase program in which the project that was previously seeking funds pays back the value of stablecoin it owes to the smart contract, including any interest owed.

Once the project has sent all funds to the smart contract, the payout redemption process can start. For this phase asset token holders of the project verify their investor keys and send in tokens to have them redeemed for Ethereum. Tokens can still move after the process is over until a chosen date. Thus, investors don't have to redeem their tokens on the first day, although they do have an obligation to redeem their tokens eventually.

If the redemption period of a project has been going for some time, CONDA will attempt to notify investors with addresses that have not yet redeemed their holdings via their CONDA account. If there are still small amounts of unredeemed Ethereum in the smart contract after another long period of time, then the original project creator can reclaim these repayments. Part of the funds will go towards research of the ecosystem.

In short the repayment process is as follows:

1. The predefined blockheight for the end of the project time is reached.

2. The project owner now has time to repay the full amount owed to the smart contract. If the owner is unable to repay the full amount through liquidation, there might be options to pay back parts of the funds equivalent to token holdings.

3. Successful projects will repay the full amount invested plus interest to the smart contract by sending asset tokens to it. This process automatically triggers a payout of funds to the sender's investor key holding address.

4. After the (long) time to redeem tokens has passed, leftover funds will get returned to the project and be partly used for research purposes.

Tokens can also be moved out of exchanges and into the smart contract after the project is over, though investors should pay attention so as not to miss the ultimate deadlines for recuperation of funds.

In case that the asset token represents a company's stocks and not debt financing, there will be no repayment process. A stock issuing company can pay out dividends to their shareholders and disclosure laws according to their local jurisdiction have to be followed.

# 4 Future Research Areas

The following are areas of research that might lead to future adaptations of the network.

## 4.1 Staking and Time-lock

Fee payment can be made in a way that aids the long-term growth of both the underlying token and the platform. Fees can therefore be paid consecutively in a streaming manner over the project's lifetime so that more tokens are locked up in smart contracts when the platform is heavily utilized. The fees a project has to pay to enter the network are proportional to the amount it wants to raise and the timeframe it plans to keep the funds. The project then stakes this amount

of fees on its account. Initially, with a lower price, this process might represent a bigger part of the total supply, but long-term, as more coins get locked up, a project can lock up a smaller overall portion of the total coin supply due to the increased price.

A small part of the staked coins is then deducted regularly for the listing platform and CONDA's network maintenance. This ensures that CONDA and the platform are incentivized to grow the network with valuable projects that are likely to succeed long-term. In the case of early liquidation, locked up coins can be used to pay for legal expenses and liquidation procedures with the aim of recuperating at least part of investors' funds. Staking can align the incentives of the stakeholders on the platform and works towards the notion that in a distributed community experiment[15] the community can work without a centralizing entity if everybody's incentives are aligned. Creating the right incentives is essential for any utility token platform to function for the long term.

## 4.2 Stablecoins

Ether (ETH) will be the currency of choice for investments on the CRWD Network for the time being. This is a bit problematic due to the volatile nature of cryptocurrencies and can only be managed with a hedge or partial sale of the currency against a more stable asset.

To avoid this in the next iteration of the network, a stablecoin should be used as a replacement for ETH. Stablecoins used or in development right now are Tether, Digix DAO, Maker DAO, Carbon or Saga, and they all have different risk profiles. While some are relatively simple and use a middleman, others are more complex and try to avoid the middleman completely through restricting and expanding the coin supply as necessary.

While these projects of are too centralized or untested for a production environment, future iterations could prove worthy of adoption by the CRWD Network.

## 5 Discussion

The CRWD Network is a step into the future of decentralized asset management, allowing individuals to take part and add value to the ecosystem by creating their own local platforms. The CRWD ecosystem can run internationally without hassle because fiat currencies are not directly involved in any steps of the process; rather, fees and investments are done through the CRWDToken or a stablecoin. The possibility to sell and buy asset tokens even before a project has ended is another incentive for investors to move to the blockchain. In terms of cost cutting decentralized systems can cut out middleman and increase

competition to push down costs even in the highly regulated financial market and therewith finally offer alternative solutions to established methods.

For the CRWD ecosystem are multiple steps to consider to further decentralize the concept. One option would be to give CRWD platforms the option to vote on the addition of new members with their platform's key signatures. This could decentralize the key handout and revocation process and would further empower the local platforms. CONDA in this case can serve less as a centralized entity in the system and more as a supplier to the ecosystem aiding it to further grow its technical capabilities.

# 6    Conclusion

Regulated legal asset tokens must have some form of centralized elements. The CRWD project minimizes those centralized touchpoints while opening up a big market for asset-backed tokens to the masses. With increasing regulatory acceptance of the blockchain ecosystem, the project leaders believe that it is just a question of time until asset-backed tokens take over vast areas of the financial ecosystem. The CRWD project can be one of the first networks to do so, letting people transact and invest freely into projects they themselves deem investment-worthy.

# Glossary

**blockheight** It is the number of blocks in the chain between the one you are viewing and the very first block in the blockchain.. 13

**carbon** Carbon is another idea of a stablecoin implementation. Details can be found under `https://carbon.money`. 14

**digix DAO** Digix is a project that recently went live on the Ethereum mainnet and uses gold in an actual physical vault as stability mechanism for its token. 14

**ethereum gas** In Ethereum, Gas is Ether (ETH) spent for a coin transfer or to create and use a smart contract. Gas has to be spent on miners to get any of these events to execute on the Ethereum blockchain. 11

**EOS** EOS is an alternative smart contract supporting blockchain using a modification of the proof-of-stake consensus algorithm named delegated proof-of-stake. 2

**ERC20** ERC20 is a standardization for a token on Ethereum and describes how this token has to function to be ERC20-compliant and therefore work with other ERC20-compliant software like wallets or exchanges. 4

**ethereum** Ethereum is an open-source public blockchain, which incorporates a smart contract scripting functionality. Right now it uses proof-of-work mining as a consensus but will ultimately fork to deploy a proof-of-stake algorithm. 2

**ethereum classic** Ethereum Classic or short ETC is a blockchain that resulted from an unplanned fork in the Ethereum community. It works very similarly to Ethereum (ETH) and actively adopts some of its new updates. 2

**fork** A hard fork of a cryptocurrency can leave a network with two different databases from this point on. If a community continues to build on both sides of the forks, both versions can be sustained, and from there on, two cryptocurrencies with a shared history exist. 3

**fundraising goal** A minimum amount of money that has to be raised so a project's fundraising process counts as successful. If the goal can't be reached, the pledged money stays with investors. 11

**KYC** Short for "know your customer", KYC is the process by which individuals' identities can by verified by requesting a copy of a legal document like a drivers license or a passport. 2–4

**maker DAO** Maker DAO creates a stablecoin that is backed by another token as collateral and restricts and adds money supply as necessary to keep it stable. 14

**NEM** Short for "new economy movement", NEM is a business-oriented blockchain solution, which uses an adaption from proof-of-stake called proof-of-importance to incentivize active usage of the technology. 2

**neo** Neo is a smart contract and token-supporting blockchain using a proof-of-stake consensus. It is popular in China. 2

**proof-of-stake** Proof-of-stake is an alternative consensus algorithm to proof-of-work and expends no energy. It uses the long-term locking of coins on the blockchain as a form of security deposit to hand out the right to write new blocks. 2

**proof-of-work** Proof-of-work is a security mechanism that expends energy and computational power to secure a blockchain. The most famous blockchain using this consensus algorithm is bitcoin. 2

**saga** The saga foundation is creating a stablecoin. Details can be found under `http://saga.org`. 14

**security token** A token that represents a security, which can be a share in or a claim against a company. 5

**solidity** Solidity is a high level programming language for the implementation of smart contracts. It's most commonly used and natively supported by contracts on the Ethereum blockchain. 3

**stablecoin** A stablecoin is a price-stable cryptocurrency, meaning it fluctuates little in value when compared to fiat. Think of it as though you could own Euro on a blockchain. 4

**tether** Tether is a centralized stablecoin related to the bitfinex cryptocurrency exchange. It holds USD as reserve to back up the value of the stablecoin. One tether historically trades around one USD. 14

**tezos** Tezos is a not yet launched blockchain using an integrated voting governance system to allow for easier hardfork upgrades. 2

**utility token** A token that serves it's utilizer a special purpose on a platform or network. The purpose it has, gives it demand or value. This also separates it from an asset or asset token which is a claim against a person or company. 4

# References

[1] Ziegler T, Shneor R, Garvey K, Wenzlaff K, Yerolemou N, Rui H, Zhang B. *Expanding Horizons: The 3rd European Alternative Finance Industry Report*. SSRN Electronic Journal, 2018. `https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-ccaf-exp-horizons.pdf`

[2] Daniel Pichler. 2018. *Tokenization The Shifting Future of Digital Assets*.

[3] Franklin Schrans. 2018. *The Flint Programming Language* . `https://github.com/franklinsch/flint` [Accessed 16 April. 2018].

[4] ConsenSys Media. 2018. *The Inside Story of the CryptoKitties Congestion Crisis*. Available at: `https://media.consensys.net/the-inside-story-of-the-cryptokitties-congestion-crisis-499b35d119cc` [Accessed 20 Mar. 2018].

[5] Ethereum Research. *Sharding phase 1 spec*. 2018., `Availableat:https://ethresear.ch/t/sharding-phase-1-spec/1407` [Accessed 16 Mar. 2018].

[6] Vitalik Buterin. *A minimal sharding protocol that may be worthwhile as a development target now*. 2018., `Availableat:https://ethresear.ch/t/a-minimal-sharding-protocol-that-may-be-worthwhile-as-a-development-target-now/1650` [Accessed 16 April. 2018].

[7] Raiden Network - Fast, cheap, scalable token transfers for Ethereum, 2018. Available at: `https://raiden.network/`[Accessed 16 Mar. 2018].

[8] Joseph Poon, Vitalik Buterin. *Plasma: Scalable Autonomous Smart Contracts*. 2018., Available at: `https://plasma.io/` [Accessed 16 March. 2018].

[9] Ethereum Research. 2018. *Plasma Cash: Plasma with much less per-user data checking*. Available at: `https://ethresear.ch/t/plasma-cash-plasma-with-much-less-per-user-data-checking/1298` [Accessed 16 April. 2018].

[10] Gibraltar Blockchain Exchange Available at: `https://gbx.gi/`[Accessed 24 Apr. 2018]

[11] Finhaven. Available at: `https://www.finhaven.com/`[Accessed 24 Apr. 2018]

[12] Fabian Vogelsteller. 2018. *ERC: Identity #725*. `https://github.com/ethereum/EIPs/issues/725` [Accessed 07 June. 2018]

[13] Fabian Vogelsteller. 2018. *ERC: Identity #735*. `https://github.com/ethereum/EIPs/issues/735` [Accessed 07 June. 2018]

[14] Conda. 2018. *Our versatile white label solution*. `www.conda.online/en` [Accessed 09 May. 2018].

[15] Matthias Tarasiewicz, Andrew Newman. 2014. *Cryptocurrencies as Distributed Community Experiments* `https://www.academia.edu/9622400/_2014_Cryptocurrencies_as_Distributed_Community_Experiments`