A Decentralized Insurance Exchange

Alan Wenyuan Sun

September 18, 2020

1 Field of Invention

This invention is a decentralized insurance exchange, in which insurance seekers can create personalized insurance policies. These insurees can then place their policies on a decentralized exchange where any individual/organization can bid to insure these policies.

2 Background

Generally speaking, insurance is a suppliers' market. Consumers are left in the dark as to how insurance plans, provided by large insurers, are formulated and priced. They also do not have the ability to modify or adjust these plans to their own satisfaction. Thus, it is difficult for consumers to participate proactively in the market of insurance. On the other hand, from the perspective of the insurance provider, information needed to accurately price the insuree's plan does not come easily. The availability of this information is often at odds with the consumers' best interests of keeping their payments as low as possible. Without this critical information, insurers must acquire this by adding mandatory disclosure clauses in the insurance contracts or infer these fields through big data collection/prediction. An excess of capital needed in addition to the information asymmetry in the market raises the barriers to entry for insurance providers. This prevents the market from reaching an equilibrium that maximizes social welfare. Therefore, there lacks a personalized, informational symmetric insurance system where consumers can contract on their terms and insurers can adequately assess the risk of their investment.

Recently, the popularization of blockchain technology has inspired many developers to create decentralized insurance solutions to the aforementioned problems. These peer-to-peer solutions crowd source insurance by organizing groups of insurance seekers by their associated communities – friends, family, co-workers. Individuals that opt-in to this type of insurance system submit insurance claims to the group. These claims are then validated through a majority vote. If a claim is validated, it is the groups' responsibility to pay out the claim. Though these proposed systems have their limitations, nonetheless, they have paved the way for this present disclosure.

3 Brief Summary of the Invention

The present invention seeks to bring personalization, security, and increased transparency to the market of insurance. This is achieved through three important components: smart contracts, the decentralized exchange, and a claim validation system. The mechanisms for weaving these components together are also a critical part of the invention.

Smart contracts are stand-ins for physical insurance contracts. These digital insurance contracts are instantiated by the insuree through parameterizing existing template contracts. In that way, even consumers who are not tech-savvy can participate in creating reliable and secure smart contracts. Clauses outlining the terms of claims and disclosure of any relevant personal information is at the discretion of the creator of the smart contract. The contract can also be refined and/or negotiated through the exchange. Past contract transactions, with private information anonymized, is also publicly available for reference by interested parties.

The newly created contracts are placed onto the decentralized exchange where insurance providers/investors can place bids on these contracts, similar to a stock exchange. On this exchange, interested parties can price their bids based on the information disclosed by the insuree. This inherently rewards insurees who disclosed as much relevant information as possible with an accurate cost of insurance, while punishing consumers who disclose no information with no bids or absurdly high cost-of-insurance. Through this process, the exchange encourages consumer discloses, aligning the interests of the insurer and the insuree.

Negotiation can also take place during the bidding process; whereby, bidders can add dimensionality to their bids in addition to the premium offered – conditions of claims, relevant service providers, the start/end date of the contract itself, and validation methods.

When the bidding party comes to an agreement with the contract holder, collateral (paid by both the insurer and the insured) is placed into the smart contract, and said contract is activated. The collateral is released when either the contract is voided, one party forfeits, or when the contract ends.

When a claim is made, it is validated through a trusted third party. This includes public databases, service providers, or government agencies. When the claim is determined valid by this third party, a payout is automatically issued to the insured party from the insurance provider via the smart contract itself. Disputes regarding the validity of claims and payouts are solved on the platform itself. This involves an on-site auditors' committee. These committees, formulated by the platform itself, serve as mediators.

The barrier to entry for insurance providers is not only hiked up by information asymmetry but also capital requirements. Thereby, this invention also allows individuals to aggregate their capital together to form larger insurance entities called mutual risk obligations (MRO). This sharing of the risk not only benefits ”smaller” insurance providers but also mitigates risk for the insuree. This makes it possible to crowd-fund expensive insurances (rocket/satellite insurance, or annuity).

Further, currently, many of the third-party professionals involved in insurance support the insurance provider. With smart contracts and crowd-sourced insurances, insurees will also be able to reap the benefits of the services provided by these professionals, leveling the playing field.

4 Brief Summary of the Drawings

Figure 1 illustrates a detailed view of the interactions between various stakeholders and the flow of currency through each of them in a contemporary insurance company.

Figure 2 depicts the proposed insurance system, the relationship between various stakeholders, and how currency flows within the invention.

Figure 3 demonstrates the process of creating a smart contract. The insured party possesses particular fields of private information and can choose to instantiate a parameterized contract with as many or as few of these fields as they want.

Figure 4 shows a mutual risk obligation, where groups of investors/insurers can aggregate their capital to ensure a large number of insurees. This minimizes the risk of insurance for the insurance provider and the insured party.

Figure 5 demonstrates the process of bidding on smart contracts in a decentralized exchange.

Figure 6 shows trust graphs between the insuree, the insurance provider, and the service provider in three types of insurance contracts – “subjective” insurance, “objective” insurance, and a MRO.

5 Detailed Summary of the Invention

5.1 Disclosure

The terminology and exemplifications used herein is to describe particular embodiments only and is not intended to be limiting of the invention. This also applies to the figures and their descriptions provided above and below. As used herein, the term “and/or” includes all combinations of one or more of the associated listed items.

In describing the invention, it will be understood that several techniques and steps are disclosed. Each of these steps has its benefit and can be used in various permutations. For the sake of clarity, this description will refrain from repeating every possible permutation of the individual steps in an unnecessary fashion. The term “etc.” is used at the end of a list to indicate that further similar items are also included in the associated listed items. For brevity, these similar items are excluded.

Nevertheless, the specifications should be read with the understanding that such permutations are entirely within the scope of the invention and its claims.

The exemplifications of the invention in the latter sections are not intended to limit the invention to the specific embodiments. This also applies to the figures and their descriptions provided above and below.

5.2 Stakeholders of the Platform

This subsection concerns itself with the various stakeholders on the platform. The present disclosure defines these stakeholders, outlines their attributes, and contrasts them with the stakeholders of formal insurance systems.

5.2.1 Insured Party

The insured party represents consumers who are looking to be insured. Note that these consumers not only encapsulate laymen but also corporations or other insurers seeking insurance. In any insurance system, the goal of the insured party is to find an insurance policy that is not only affordable but covers all of their needs. The insured party is also seeking a reliable insurance provider – providers that offer stability[1]. Consumers generally have a plethora of data about themselves including contact information, social security number, birthday, health history, pre-existing health conditions, travel history, daily routines, etc. Since it is in the consumers' best interest to have as low a premium rate as possible, they will be reluctant to reveal any “harmful” information[2]. This creates a problem for the insurance provider as the amount of information available is negatively correlated to the risk that the insurance provider bears. With more information, insurance providers will be able to more accurately gauge the cost of insurance.

Currently, autonomous insurance seekers, who do not have coverage associated with an employer, need to potentially look through tens of plans to determine which policy is best. As depicted in Figure 1, many insurance policies are pre-determined by insurance providers, then retailed to insurees. Rarely do consumers have the opportunity to make modifications on top of these template

[1] Providers who issue payments or reimbursements to valid claims in a reliable and timely manner.

[2] Information which would make insurers flag them as “high risk,” which would in turn drive up premiums.

plans. After accepting a generic plan, the contemporary insurer would then impose an adjustable rate premium – as to mitigate the risk brought on by the informational asymmetric insurance market. These adjustable-rate premiums depend on many factors that are generally affected by the claim rate of the insured party.

The proposed system lowers the barrier to entry for insurance providers. In that sense, it decreases the insurees' dependence on a particular insurance provider. This invention makes the insured party responsible for defining their insurance policy. The insured party can define what it is that they wished to be insured for, specifically what conditions must be met for payments to be made, as well as the service providers responsible for validating their claims. These self-defined policies along with any personal information the insured party wishes to disclose are stored in a parameterized smart contract and placed onto the open marketplace for bidding. Policy-creators can also reference existing policies on the market, or they can hire experts/professional to assist them in creating these contracts.

In this way, consumers can guarantee that their self-created insurance plan covers all of their needs. Assuming that there exists an adequate number of competing insurance providers on the decentralized exchange, their self-defined plans will be priced appropriately based on the plan itself and the quality/quantity of the information they choose to disclose. In this sense, as the numbers of users increase the market will become increasingly informationally symmetric and efficient. Bidding on the decentralized exchange is described in detail in 5.3.2.

Traditionally, consumers are more likely to flock to large insurance providers. The plans that these mainstream insurers offer are more cost-effective and it is easier to trust a large insurer – whether that be because of a namesake or other factors. The imposition of smart contracts chained together in a blockchain prevents insurer fraud, as once claims are validated the smart contract automatically executes and the insurer is bound to pay. A collateral payment – agreed upon the contract's activation – from both the insurer and the insuree acts to further de-motivate fraud. This decreases the need for trust within the system and gives insurees the possibility of signing with a lesser known insurer. This is further discussed in 5.4.1.

5.2.2 Insurance Provider

The insurance provider represents consumers and/or corporations and/or organizations who are looking to insure the insuree. To mitigate risk, it is advantageous for insurance providers to insure many entities at once. It is the insurance providers' responsibility to perform risk assessments on each of its investments. Through premium payments, insurance providers commonly have large amounts of capital at their disposal. This is often invested in financial markets, which would give insurance providers a source of passive income.

For the insurance provider to become lucrative, they need to reduce the collective risk of their investment. This is done by insuring many simultaneously. Due to the large required starting capital for insurers, there is a high barrier to entry. Thus, insurers are generally massive corporations. This barrier to entry is exacerbated through the aforementioned problem of asymmetric information disclosure.

The insurance provider is responsible for claim validation – the determination of fraudulent insuree claims. This involves corroborating with service providers. Traditionally, since there needs to be trust between the service provider and the insurer, these two parties often form collusive conglomerates. This often presents a problem for insurees as service providers might not be acting in the best interest of the consumer.

This invention simplifies the responsibilities of the insurance provider. Firstly, with parametrized smart contracts, the insurance provider no longer needs to probe consumers for information, as it will likely be disclosed by the consumer. Insurance providers can use this to their advantage by directly using the quantity of information supplied as a risk assessment factor. Insurers can label those who provide little to no information as "high-risk," while consumers who disclose more information are likely to be priced accurately. These risk assessments should factored into the offering price by the insurer. Secondly, as depicted in Figure 4, insurance providers who have little capital can band together in a mutual risk obligation. Together, these smaller insurance providers can aggregate their wealth and "diversify" their risk. Finally, the responsibility for determining the validity of a claim is placed onto the service provider and the oracle, outlined in 5.3.3. These factors make becoming an insurance provider easier. Thus, laymen can now participate in the decentralized exchange as an insurance provider. The similarity between the insurer and insuree demographic is represented in the module label "Consumer (Insurance Provider)" module in Figure 2.

In the proposed system, insurance providers are still able to invest their capital into financial markets by exchanging the platform's cryptocurrency for real dollars. For insurers participating in a mutual risk obligation, a new smart contract can be created which specifies how the return on financial market investments is to be distributed among its shareholders.

5.2.3 Service Provider

The service provider provides the insured service to the insuree. Depending on the type of insurance, the service provider may or may not exist. For example, life and weather insurance do not have service providers. In such applications, where the validity of a claim cannot be validated by an appropriate service provider, an external trusted third-party source is consulted. This includes cross-referencing reports from the national weather service with local weather reports or matching death certificates with federal databases. The action of cross-referencing/matching with a third-party database is the role of the oracle, which is discussed in detail in 5.2.5. The cross-reference source needs to be chosen and agreed upon by both the insured party and the insurance provider.

On the other hand, where there is a clear service provider in the case of health insurance or car insurance, these service providers are responsible for determining the validity of the insurance claim. As shown in Figure 1, traditionally the service providers are coupled with the insurer. The interactions between both parties reduces the need for dialogue between the insured party and the insurance provider. Moreover, this coupling encourages trust between the insurer and the service provider – the insurer brings the service provider business, while the service provider validates claims in the best interest of the insurer. In this way, insurers can reduce the risk of insurance by only covering services provided only reputable and "trustworthy" service providers.

The contemporary insurance system encourages collaboration between the service provider and insurer; often the consumer is at a disadvantage: they do not have many options with their insurance policies or service providers. Moreover, smaller service providers are discouraged to enter the market, because large insurers are more likely to couple with large service providers. This bond takes away business from "up and comers" since consumers are forced to use services from these large service providers.

This invention mitigates these problem in two ways. Firstly, it allows the insured party to choose their service providers. This interposes the dependency of the service provider on the insurer. Further, this would give the insured increased access to the services that they are comfortable with. Secondly, the insurance provider no longer needs to explicitly trust the service provider. Rather both parties – the insurer and the insuree – can assess the credibility of the service provider by analyzing available public information. This public information is published both by the service provider themselves and the platform. Exemplifications of information that could be collected by the platform are fraud rate, customer satisfaction, insurer satisfaction, cost of service, and/or the number of clients who are also being insured by those on the platform. These statistics are then aggregated into a rating.

Service providers respond to claims with digital signatures, which are then passed into the oracle. If the signature matches the service provider's signature in the smart contract, then the claim in question is validated. The service provider's independence from the insurer is an added risk for the latter. Thus, the risk of a rogue service provider is mitigated through on-site, third-party auditing, as well as the due diligence of the investor. The digital signatures which give service providers the power to validate claims are awarded only after on-site auditing is complete.

Third-party auditing is the process by which a group of users, composed of equal demographics of insurers and consumers audit service providers for a fee. This is comparable to the risk assessment module depicted in Figure 1. When a service provider applies and after all information relevant information is reviewed, a majority vote is held. The result of this majority vote determines the status of the service provider's application. If a majority votes for the approval of the service provider, the service provider is issued a digital signature and now can validate claims. This approval status will also reflect on the service provider's profile. The formulation of this committee is furthered discussed in 5.3.3. Service providers are also tagged with unique identifiers – separate from the digital signature – which also prevents imitation.

Service providers can share information about themselves across the platform including the number of clients they are managing, age of the establishment, investors/interest groups, images of the establishment, and/or licenses from the government. Supplementary material of the images of these licenses can be included as well. These supplementary materials will also help the auditors' committee and other insurers on determining the integrity of the establishment. As mentioned before, the invention itself would also be able to generate a credit-score-like rating for each establishment, which should further inform the fraudulence of the service provider. This credit-score-like rating can also be corroborated with reviews and ratings from the insurance providers and the insurees. Since it is in the best interest of service providers to attain a digital signature – so they can start validating claims and accepting business – disclosing as much information as possible about themselves will only increase their chances of being awarded a digital signature.

Alternatively, if a service provider has not yet been issued a digital signature, the insured party and the insurer are still able to choose this establishment as the primary service provider of the contract, at their own risk. The "high-risk" service provider will be issued a pseudo-digital signature – a one-time signature used for validating claims in this particular contract.

If there is a dispute between the insurer, service provider, and/or the insured party, the case is handled internally by the auditors' committee outlined in 5.3.3. All information about the insurance provider, the claim, service provider, and relevant supporting materials is submitted to the group and a majority vote acts as the ruling of the dispute.

5.2.4 Reinsurer

As shown in Figure 1, the reinsurer insures the insurance provider. In the proposed decentralized exchange, the reinsurer also corresponds to the insurance provider of the insurance provider, the role of these two parties mirrors the relationship between that of the insured and the insurer. For the reinsurer, however, validation is made easier. Since all of the insured parties' – the insurance provider who is being insured – contracts are on the blockchain, the oracle can easily traverse the blockchain to validate the claims from the insurance provider being insured.

Similar to the insured party, this new insured party – the insurance provider – is also able to create smart contracts that describe all of the assets that they wish to be insured. Reinsurers can bid on these contracts as described in 5.2.1 and 5.3.2. It also should be noted that the reinsurer is not limited to a single entity. The insurance seeker – again, which is the insurance provider – can package their contract into an MRO (mutual risk obligation), which allows many reinsurers to share the risk of the investment.

5.2.5 Oracle

The oracle is defined as a digital entity that controls the payouts of smart contracts. Since neither blockchains nor smart contracts can look beyond the information they already possess, the oracle is a mechanism by which external data can be fed into the blockchain so that smart contracts know when to execute. The oracle itself has no biased interests as its actions are determined algorithmically. The oracle can acquire data required by the smart contracts through three ways:

1. The oracle checks external APIs and/or public databases.

2. A service provider/insured party feeds data into the oracle.

3. The oracle traverses the blockchain itself to gather data.

The first case follows that no service provider is available to provide claim validation information. This case is also true of a financial market reinvestment smart contract – the oracle would gauge the status of the market and partition the returns based on the conditions of the contract. In the former case, the oracle needs to verify claim information by searching through online databases. The databases/APIs which the oracle uses in such cases are agreed upon by the insured party and the insurance provider.

In the second case, a service provider is present. When a claim by the insured party is made for reimbursement, a request for a digital signature is made by the oracle to the service provider. Alternatively, the claim can also be filed by the service provider. In this alternative case, the oracle would request a digital signature from the insuree.

The third case follows applies to the reinsurer. The oracle is simply traversing the blockchain and peeking at blocks ahead or behind the current block to validate/falsify the insuree's claim.

5.3 Processes of the Proposed Platform

This subsection is concerned with the various interactions between stakeholders on the platform. It is divided into four crucial operations that users of the invention will likely use: Creation of Smart Contracts, Bidding in the Decentralized Exchange, Claim Validation, Staking and Bundling Risk, as well as Reinvestment.

5.3.1 Creation of Smart Contracts

This section describes the creation of smart contracts. The process of instantiating a smart contract is demonstrated in Figure 3. The illustration shows a particular user creating a health insurance policy. The information in the cloud represents all of the information that "John" knows about himself. The user can choose which of these fields to disclose and which of these fields to keep private. The parameterized smart contract shown in the box "Parameterized Contract" represents the minimum information required for a smart contract: covered services, claim validation method(s), premiums/cost of insurance, collateral from the insurance provider, and the insured party, toggling of cash-value cancellation. The other three fields: claim, report fraud, and re-negotiate terms represent an excerpt of the methods available in the smart contract. These parameterized smart contract are an interface that provide basic functionalities so that the users does not need to make up their own from scratch. Users with more experience can create their own smart contracts with customized functionalities as well.

When a user creates a smart contract they are instantiating this parameterized smart contract with their information. Depending on the type of insurance, the functionalities of the smart contract could change. For example, contracts for health insurance might allow users to update or change their service provider or upload relevant claim information that includes multi-media.

The user then inputs basic parameters along with any other information that they wish to disclose. Personal information disclosed in the smart contract is at the users' discretion. Users can also choose to "coarsen" sensitive information; for example, in Figure 3, John's age after coarsening would become "45-55." The level of coarsening is decided by the user. This ensures a level of anonymity and privacy while still providing adequate information.

During the instantiation of such smart contracts, users can invite institutions to issue digital signatures to verify the information the inputted information. Verification may also come in the form of triangulating the uploaded information with public records.

Another method to increase user integrity is to mandate identity verification at the inception of the user's account. This alternative method reduces the overhead present in the previous method.

The identity verification process can be performed one of two ways. Either the appropriate institution can issue a digital signature, or the oracle can cross-reference these fields with public databases upon adding these contracts to the blockchain. To expedite the process, the insured party/insurance provider could also provide images of their associated documents. The visibility[3] of the uploaded information is at the user's discretion.

After the user creates their smart contract, the contract is placed on the decentralized market for bidding. Only when the insured party and the insurance provider agree on the terms of the contract does the contract become active, initialized, and added to the blockchain.

The insurance provider is also able to re-insurance their smart contracts by creating smart contracts through the same procedure described above.

Smart contracts can also be linked together in clusters. These clusters are named MROs (Mutual Risk Obligation), described in section 5.3.4. These contracts are created for the purpose of either bundling risk or investing in financial markets.

5.3.2 Bidding in the Decentralized Exchange

Individuals and/or organizations who create smart contracts can place these contracts on the decentralized exchange where prospective insurers can then bid on these contracts. The smart contract creator can decide the criteria of bidding as well as the mode of bidding itself – including open, silent, or hybrid. During an open auctioning process, all bids are public. Conversely, during a silent auction, all bids are private. A hybrid auction shows bidders the current lowest bid offered. This is neither a comprehensive or exhaustive list of the different modes of bidding processes/criteria available.

Figure 5 shows the various commodities available for bidding on the exchange. The bidding of MROs come in the format of price per share, while the bidding of individual smart contracts come in the form of a single price. In the case of an MRO – where there are potentially hundreds if not thousands of shares – sellers can set a fixed price and then create an initial offering on the market place. Further, bidders who are bidding on "regular" insurance contracts can add dimensionality to their bids. In addition to offering a premium, insurance providers are also able make their offer more attractive by adding cash value cancellations or other perks. The insurance provider and the insuree may even negotiate eligible service providers and the terms of the contract during the bidding phase.

The creator of the smart contract is also able to add exigence to the bidding process by enacting a valid bidding period. Bidders are also able to create urgency in their bids by adding a time limit on their offer, such that when the time ends the offer is rescinded. Bidding is terminated after either the creator picks an offer or manually decides to terminate the process. The contract then becomes active with the conditions that both the insurance provider and the insured party agreed to during the bidding process.

Shares of an MRO can be traded without limitations. However, the ability for insurers to resell a contract not categorized as a MRO is determined by the insured party – enabled during the creation of the smart contract. During the reselling of a classical insurance contract, the terms of the contract that were initially agreed upon are upheld. These terms include the collateral, specified service providers, claim validation method, and so forth. When such a contract is resold, the collateral belonging to the seller is only released when the buyer places the insurer's collateral into the contract. Before the collateral is transferred and replaced, the seller still bears full responsibility of the contract.

On the other hand, shares of an MRO can again be placed on the decentralized market where they can be resold with the same procedure described above. Shares of an MRO can be bought, sold, and resold without the same restrictions as classical insurance smart contracts.

5.3.3 Claim Validation

A claim is submitted to the platform when the insured party believes that the claim meets the claim conditions outlined in their insurance smart contract. The process of claiming varies based on the type of smart contract and the inherent nature of the party/service being insured. The three types of claim validation methods are outlined below:

1. The contract does not or cannot have a well-defined service provider (e.g. life insurance, weather insurance). Since such claims cannot be verified by a service provider, the oracle – defined in 5.2.5 – references a third-party, external dataset. The dataset is agreed upon between both the insured party and the insurance provider.

2. The contract has a well-defined service provider. In this case, the service provider issues a digital signature that validates the claim. On the other hand, if the service provider has not been awarded a digital signature, then a one-time, pseudo-digital signature is created for this service provider to authenticate the claim.

3. The contract does not have a well-defined service provider, but the claim can be validated by traversing the blockchain. For example, smart contracts insuring other smart contracts can be validated by simply traversing through the blockchain and examining the payouts of the insured smart contracts.

Both the operations performed in the first and last processes outlined above are trivial cases described in 5.2.5. Note that in all three cases, if the insured event occurs, the user should proactively make a claim. If a claim by the user is not submitted to the platform, no payout is considered, even if the claim condition is met – this is true of all three conditions. In the second circumstance

[3] The ability for other users to see the content uploaded by the user in question.

where there exists a service provider, the service provider must corroborate the claims of the insured party.

A service provider can only authenticate a claim with a digital signature. The process of a service provider acquiring a digital signature is discussed in 5.2.3. This digital signature must match the digital signature provided in the smart contract. When an invalid digital signature is detected, this registers as an attempt at fraud from the malicious service provider and the service provider is *flagged*[4] When a claim is validated, the claim amount is either reimbursed to the service provider as a result of the service, or it is returned to the insured party.

If a claim is disputed between the insurer and the insuree, the dispute is mediated by a group of auditors hosted on the platform. Most often the group will decide the outcome of a dispute through a majority vote. The types of disputes that are likely to occur are listed below; Note, this list is not exhaustive.

1. A claim is determined to be valid by the service provider, but the insurer simply will not payout the deserved amount.

2. The insurer argues that the claim is not valid. This may be a result of suspected collusion between the service provider and the insuree (conflict of interest).

3. The insuree asserts that the claim is valid, but the service provider, for whatever reason, will not grant a digital signature to activate the payout in the smart contract.

4. Either party suspects that there is collusion or a conflict of interest between the other two parties.

5. When the claim amount is greater than the collateral, so the insurer abandons the smart contract, leaving the insuree at a deficit.

6. Both the insuree and the insurance provider acknowledge that the claim is valid, but there is a dispute regarding the valuation of the claim.

7. The insured party is unwilling to pay the premium agreed upon the creation of the contract.

Since ambiguity is most likely to arise when a service provider is involved or subjective evaluation is required to evaluate a claim, the above scenarios are most likely applied to the aforementioned second enumerated case. In rare cases, claim valuations may be disputed in the aforementioned first and last enumerated cases.

Case 1 occurs when the claim made by the insuree is determined to be valid by the service provider; however, the insurer, refuses to pay out the agreed-upon amount. This most general case is settled by passing all relevant information and materials to the claim auditors. Given this relevant information, the claim auditors propose solutions to the dispute. The outcome of the dispute is then determined through a majority vote by the auditors. When the dispute is settled by the auditors, a fee is charged to either the plaintiff or the defendant based on whomever the outcome is favored towards. This fee is split among the auditors equally. If the case is overturned, or if the ruling is indecisive, the party which brought the case to attention is responsible for this fee. If a party will not adhere to the ruling or pay the appropriate fees, they are flagged and prevented from further transactions until the debt is paid off. Interest rates may also apply to any outstanding debts.

Case 2 arises when a claim is validated by the service provider, but the insurer claims that the approved claim is not valid. Similar to 1, all relevant materials and information are sent for review by the auditors. If a verdict is made that determines collusion between the insuree and the service provider, both parties are flagged which will inform future investors of collusion. Moreover, the insurance provider would be compensated for any damages. It should be noted that since these "auditors" do not have the legal power to subpoena either the insuree, service provider, or insurance provider, the auditors are not entitled to information. Thus, withholding information could be used as a criterion for a verdict.

Case 3 occurs when the insuree asserts that their claim is valid, but the service provider will not supply a digital signature affirming the payout. This scenario is similar to 2 and is handled as such, with the insurer and service provider as defendants.

Case 4 is a subset of the previous three cases, where there is suspected collusive fraud between the service provider and/or insured party and/or insurance provider. In this case, relevant information is submitted to auditors and a verdict is made as in 1. The parties involved in collusion may have their transaction rights revoked and damages are paid out to the affected party/parties, interest rates may also be applied to these outstanding debts.

In case 5, the collateral in the smart contract belonging to the insurer is released to the insured party. The amount of compensation given to the insuree is agreed upon by both the insured party and the insurance provider, during the creation of the contract. A censure may also be placed on the insurer and all transactions may be discontinued until any outstanding debts are settled. Note that in the case that the insurer "disappears" from the platform, the insuree can pursue legal action, under the UCSPA (Unfair Claims and Settlement Act) assuming that the identity of the insurer is known. The choice to associate with an insurer with a validated identity is determined solely by the insured party. Thus, 5 represents an outstanding risk to the insuree. The risks associated with the insured party are further outlined in 5.4.1.

[4] The user's conduct is reported to the auditors and/or administrators of the platform. When this occurs the violation will be a permanent part of a the offending user's profile. So that when future transactions are made, investors will be able to accurately gauge the risk of this individual. Other consequences include suspension of all transactions or the suspension of the user's account.

Case 6 occurs when the validity of the claim is acknowledged by both parties, but there exists a dispute regarding the specific amount of payout insured by the insurance provider to the insuree. When both parties cannot come to an agreement, the case and any relevant information are given to the auditors. However, in doing so, the insurer and the insuree implicitly accept the outcome determined by the auditors and in doing so give up their right to further negotiate. The remaining mediation process of this case follows 1.

Case 7 arises when the insured party is unwilling to pay the premium specified in the smart contract. This case is mediated in one of two ways. If collateral is specified in the contract, then all of the collateral is released to the insurance provider and the contract is voided. Otherwise, if there is a condition that specifies the consequences of a party backing out of the contract that consequence is exercised, whatever that may be. In the case that neither of the former clauses exists in the contract, the smart contract is simply voided.

The aforementioned auditors of the platform are chosen through four alternative methods:

1. Random selection
2. Voluntary registration
3. Jury-style selection
4. All-platform vote

During a random selection process, a random group of individuals is selected based on their interests and "party" affiliation. The auditor's group is randomly selected such that each demographic is equally represented. This selection process can also involve auditing the candidates' transaction histories to prevent fraudulent accounts from being voted into the committee. The size of the group should also be sufficiently large 100+ individuals. This committee can either be formulated *ad hoc* or permanently. In the case that the committee is formulated *ad hoc* a smaller group of 20+ individuals should do. This should effectively speed up the process of dispute settlement. On the other hand, if the group is to be formulated permanently, a much larger group is needed. Any individuals on the auditors' committee can choose to step down from the committee at any time. The random selection process would refill their seat. The total number of the permanent auditors' committee, α, that exists on the platform is expressed as a function of the number of users on the platform, N:

$$\alpha = \log \binom{N}{2}. \tag{1}$$

Eq. 1 services as a general guideline as to how many committees should be formulated on the platform at any given time. The size of each α is also dependent on N.

In the second alternative method of voluntary registration, users would register their accounts and fill out their personal information with the intention of being part of the auditing committee. The personal information provided such as name, address, social security number, and so forth need to be corroborated by an authoritative third party. This selection process is vulnerable to biased sampling, which may result in one demographic staking a majority on the committee. This could potentially create conflicts-of-interest problems.

The third alternative method of "Jury-style selection" mimics courts of law where a jury is selected and both the plaintiff and the defendant question jurors and strike out those with explicit/implicit biases. On the decentralized exchange, such committees would be chosen *ad hoc* through random selection. Then, the two parties involved in the dispute can make modifications to the jury by arguing that particular individuals are biased. It should be noted that ultimately this third style is predicated on a hierarchy of auditor's committees which oversees the formulation of other committees.

In the fourth alternative method of "All-platform vote" every individual on the platform is given a chance to vote on particular issues. Those who choose not to vote suffer no consequences. Users who do choose to vote on such issues are given a small monetary reward.

Lastly, it should be noted that in all four of these alternative methods, the voting records of a user is public and will be a part of the public record. In all cases, this public record will reveal interests or biases and can be used to determine auditor's committees in the future. Moreover, all four of these methods can either establish committees permanently or an *ad hoc* basis.

5.3.4 Staking and Bundling Risk

Barriers-to-entry for insurance providers are further lowered through staking and bundling. Insurance providers with a wealth of capital can buy insurance contracts and bundle these contracts up into an MRO. They could then sell shares in this bundle for a profit. On the other hand, insurers who do not own much capital but still want to insure can buy shares of these bundles. In this sense, investors can easily own shares of many contracts at the same time, effectively lowering the risk of their investment without needing much capital or research. *Bundlers* who create MROs correspond to the agents and brokers contemporary insurance systems described in the "Delivery Channel" module in Figure 1.

The aforementioned bundles are named Mutual Risk Obligations (MRO). MROs are simply insurance smart contracts within insurance smart contracts. The burden of payout – to the insured party – and the premiums that are paid to the shareholders are both distributed based on the percentage ownership of the MRO. After acquiring one or more smart contracts – the bundler would acquire these contracts through the aforementioned bidding process – the bundler is then able to create a new smart contract encapsulating all former contracts. This smart contract specifies the payout scheme of the contract as well as any relevant information regarding its constituent contracts – this process is similar to the described procedure in 5.3.1. After the smart contract is constructed, it is then placed on the decentralized market for an initial offering. This bidding process is the same as 5.3.2. Prospective insurance providers will still need to perform their risk assessment of the MRO. During this bidding process, the bundler bears the risk of any unsold shares in the contract. This means that any valid, outstanding claims in the shares held by the bundler must be paid by the latter.

An MRO can be conceived through many methods – the following listed methods are not exhaustive, rather a vast generalization of all the possibilities:

1. A specialized bundler with a wealth of capital can buy and own several smart contracts, then package them into an MRO. Positions in the MRO are then retailed off to other investors through the aforementioned processes.

2. Groups of individuals looking to be insured can band together and create an MRO themselves. The MRO is then either sold to a bundler, or shares of it can be placed directly on the decentralized market. The dynamics of this particular design is illustrated in Figure 4.

3. Individuals create their smart contract with the intention to be a part of a MRO. This circumstance is differentiated from 2 in that these groups may not have a prior associations.

The described process in 1 is applied when smart contracts are merged into an MRO after these smart contract have already been activated. In this case, the bundler must bid for each contract in the MRO as described in 5.3.2. The associated collateral and terms need to be paid and corroborated by both the bundler and the insuree. After this transaction is completed, the bundler bears full responsibility for the claim payouts of this contract. When a bundler sells a share of the MRO to an insurer, the insurer must not only cover the bundler fee, but also pay a share of the collateral specified by all of the contracts. When such a transaction occurs, a share of the collateral – originally covered the bundler – is released back to the bundler and replaced with the collateral payment from the insurer.

Method 2 is used in the context of an organization looking to ensure its constituents. In this context, it is preferable from the organization's perspective to ensure all of its employees under the same provider, such that the cost is consistent across the board. Thus, the organization can create *template contracts*[5] and distribute these contracts to its employees. These template contracts include the basic services and/or benefits that should be covered. The organization can also specify specific service providers in these template contracts. Once the template contract is created the organization can specify a collective collateral as well as provide information regarding the number of individuals being insured, organizational information, etc. The organization also has the choice to add more specific information about each individual being insured; the provided fields can undergo coarsening, as described in 5.2.1, at the discretion of the organization.

When an organizational MRO is placed on the market, the creator can sell its shares at a fixed price. During this initial round of offering, the collective contract is not activated until a majority of the shares have been sold. If an investor of an organizational MRO wishes to sell their stake in the contract, the process described in 1 is repeated.

Transactions with these organizational MROs can be done with or without a bundler. The organization can choose to pay a bundler to distribute shares of the MRO instead of retailing such shares themselves. In this case, the bundler pays all of the collateral and all contracts are active. During this time, when the bundler has not alleviated themselves of these active shares they are still responsible for the claim payouts.

Lastly, 3 outlines the case when individuals, not belonging to an organization, create a smart contract with the intention of having it be a part of a MRO. The fields in the contract are created as in 5.3.1. In this case, the contract is not active until all of the collateral in the contract is paid off and all of the shares of this individual's contract are sold. Individuals who create this type of contract can decide whether or not they want the bundler to bear the risk of the contract while the bundler is looking for retailers. In such cases where the payment of the collateral is deferred, this collateral will only apply after the bundler has sold all of the shares of the contract.

Once an MRO is created and the shares of the MRO are sold to insurers, the terms of the individual contracts composing these MROs cannot be changed unless there is unanimous agreement among all stakeholders – the insured party and all insurers of the contract.

It is also possible that an MRO is created out of a single contract. In this case, the creator of the contract would accept multiple bids, during the bidding process, on a single contract with the intention that these bidders would agree to an equal stake in the contract. Conversely, once an investor secures a contract they can also invite other investors to share the risk of this single contract at the discretion of the insuree. Along this thread, creators of an MRO particular ones in 2 can sell shares of their MRO to multiple bundlers in hope of a faster retail rate.

5.3.5 Reinvestment

In contemporary insurance systems, insurers reinvest the premiums collected from insurees. This particularly true of insurances that have rare claim events; in such

[5] A insurance smart contract where the information regarding collateral, service providers, and insurance type stays constant and only minute details regarding the individual being insured is modified.

insurance, the insurance provider does not need to fret about the liquidity of their reinvestment assets. In this way, the insurer not only profits from the claim rate to premium ratio, but also the reinvestments made using the same premiums. The insuree is "cut out" from the latter form of reinvestment.

The present disclosure gives insurees the possibility of participating in reinvestment by investing their collateral and potential claims.

Assuming that the insuree and the insurer agree, the collateral in the smart contract from both parties can be invested into other insurance contracts. This avoids idle collateral. Through this process, the return on investment of these reinvestments serves as a replacement of the collateral. Note that this reinvestment is performed at the risk of both the insurer and the insuree. The parties can either perform joint investment, aggregating their collateral together, or reinvest separately.

In the latter case, the insurer and the insuree collectively agree to reinvest the potential claims. For example, the insurer would invest the insuree's premiums into other reinvestments, similar to contemporary insurance mechanisms. However, the insuree bears the partial risk of the reinvestment as if the reinvestment results in a loss, then the value of the claims also decreases. On the other hand, if the reinvestment results in a gain, then the value of the claims would increase. Similarly, the same mechanisms also apply to the insurer. If the reinvestments result in a gain, and the claim rate is lower than anticipated, the insurer not only profits from the difference between the aggregate claim amount and the aggregate premium amount, but they also profit from this additional reinvestment gain.

The two outlined reinvestment processes can also be encapsulated in a single smart contract that automatically partitions the payouts based on collateral contribution, as well as claim validation.

5.4 Risk, Trust, and Security in the Proposed Platform

This subsection describes the risk that various parties bear while using the invention. It also describes the relationships of trust which are present in the invention and how it differs from traditional insurance. Lastly, the subsection outlines the digital security that enforces/relieves trust from the platform and how it functions to protect users.

5.4.1 Risks

The principal risk that all users bear is the risk of investing in the platform itself. All of the transactions described herein and in the previous sections are predicated on the platform's cryptocurrency. Thus, the risk that all parties implicitly bear when exchanging on the decentralized exchange is the unpredictable, fluctuations of the cryptocurrency itself. Another concern that arises immediately with the use of cryptocurrency is its liquidity. However, over time as the platform acquires more users and transactions become more frequent, theoretically, the aforementioned risk will be mitigated.

By engaging in the platform, users are accepting the risk that legal action in some cases cannot be pursued. If there is significant damage to one party as the result of collusion between other parties, all parties need to trust the decision of the auditors' committee. Further, if such losses cannot be recouped the inherent anonymity granted to users on the platform makes it so that legal action, in some cases, cannot be materialized. Thus, when buying/selling users should be wary of proper identification of the users they are doing business with[6].

Specifically, since the invention intends to achieve a perfectly efficient market for insurance, insurees with risky preconditions who benefitted from traditional information asymmetric systems may be subject to higher premiums.

5.4.2 Digital Security

The digital security in the platform ensures payouts for valid claims, prevents user imitation, and also ensures that insurers are paid the premiums they are entitled to. These features are provided through the four following components:

- Smart contracts
- Digital signatures
- The oracle
- The cryptocurrency powering the platform and its associated blockchain.

Smart contracts, digitally bind the associated parties together in the blockchain. This allows payout for both the insured party and the insurance provider to be quick and effortless, assuming that the claim has been validated through the claim validation process described in 5.3.3. Since the execution of a smart contract depends solely on the oracle there is no risk of a payout being delayed or terminated by the owner of the platform.

The digital signature component of the invention prevents with malign intentions from individuals imitating service providers. The private key issued to each service provider is encrypted with the SHA-256 algorithm. For a signature to be determined valid, the input private key after encryption by the SHA-256 algorithm needs to match the signature in the smart contract. Though digital signatures are mainly used by the service provider to authenticate claims, the insuree and the insurer also have digital signatures, which are used to affirm the transactions of smart contracts. Since the SHA-256 is computationally impossible to "break" the digital signatures ensure that

[6] Bluntly put, "seller/buyer beware."

the identity of an individual cannot be assumed by another user.

The oracle acts as an impartial digital entity that monitors the blockchain. It is responsible for the payout of the smart contract and in some cases the validation of claims. The oracle is a central part of the proposed decentralized exchange, as it prevents the host of the platform from interfering/meddling with the smart contracts or the payouts of a contract. However, if the oracle is accessing third-party services it could be the subject of ”man-in-the-middle-attacks” – where the attacker interposes the connection between the oracle and the third-party service and sends the oracle faulty information. Thus, to prevent such attacks, multiple data-inbound oracles can be used in conjunction. This would allow all of the oracles to corroborate information between various sources. Only when a consensus is established does the oracle activate/deactivate a smart contract's payout mechanism.

Lastly, the use of a cryptocurrency to power the transactions described herein is crucial for establishing decentralization. The blockchain not only provides inherent security and anonymity but also clarifies transactions between individuals through a public ledger.

5.4.3 Trust

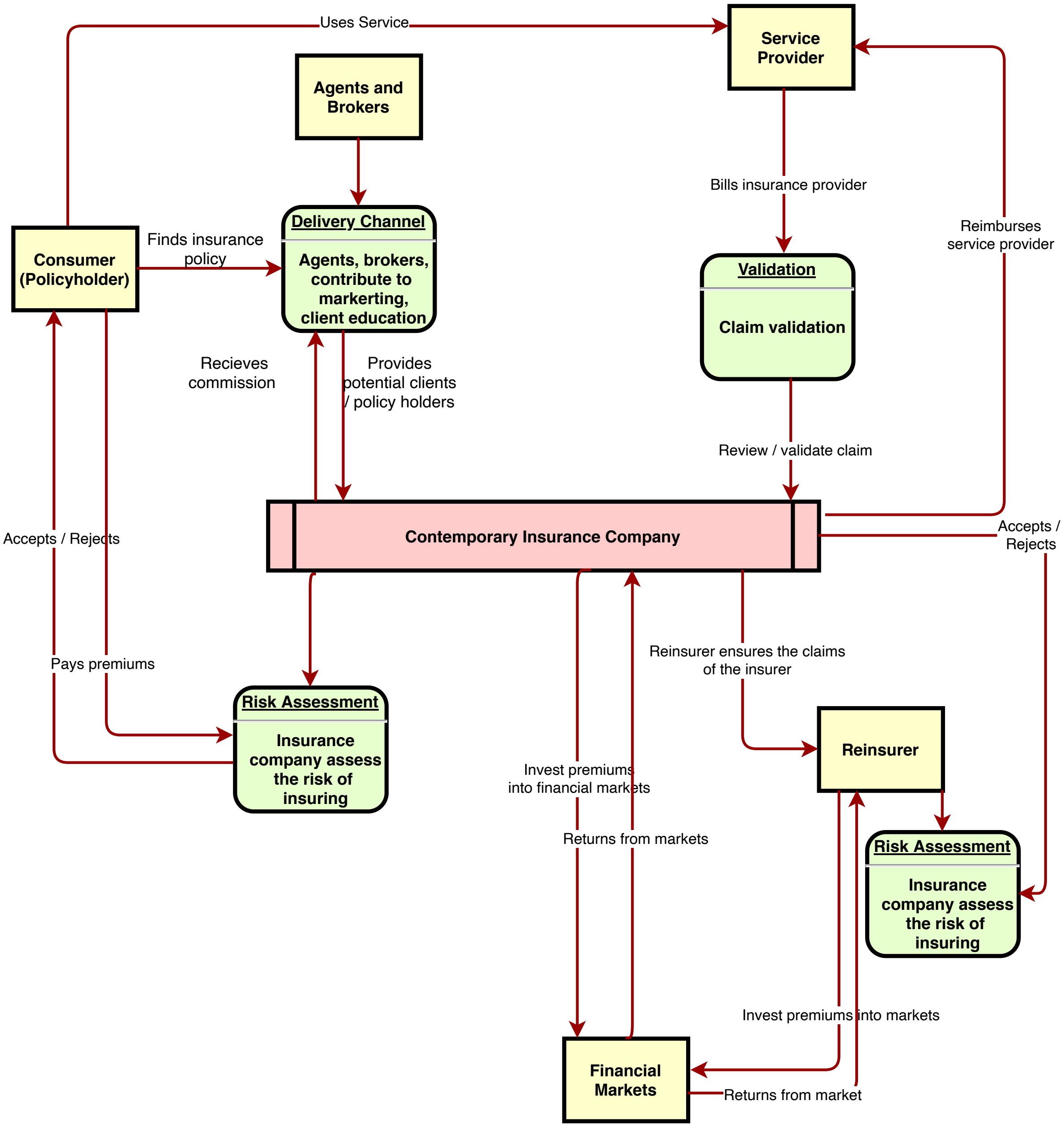
As a result of the risks discussed in 5.4.1 there needs be to trust that no collusion is occurring between any of the parties that would result in a conflict of interest. This trust between the service provider, insuree, and insurer would only be necessary for insurance contracts where the validity and valuation of a claim need to be verified by a service provider. This particular case is illustrated in Figure 6 shown in the diagram "Subjective Insurance." Note that in such a contract, there not only exists trust between the insurer and service provider, the insuree and service provider, but also trust from the insuree that the insurer will not simply abandon the contract.

In the case of more objective insurances (weather insurance, life) where it is difficult to debate the validity of a claim an oracle removes the need for trust in a service provider. Rather, there needs to only exist trust for the authoritative source selected by both parties. This relationship is shown in Figure 6, in the diagram "Objective Insurance." Additionally, in the diagram, there are no connections between any of the stakeholders and the oracle because the oracle is programmed to act algorithmically, thus explicit trust does not need to be placed in it.

Lastly, the trust that exists in an MRO is shown in the diagram "MRO," in Figure 6. Assuming that the MRO is made up of "subjective" insurance contracts, the trust graph is similar to the subjective insurance trust diagram. However, in this new MRO diagram, there exists further trust between insurers that all of the insurers insuring the MRO will bear the burden of valid claims. There also exists trust between all insurees that each insuree will pay the agreed upon premiums. In the case where there is a violation of this trust, violators will be removed from the MRO and the violators' shares/collateral will be distributed among the other investors. Note that in a MRO, the amount of trust placed on the service provider is reduced. There now only needs to be a majority of non-fraudulent service providers/insurers/insurees for the MRO to function as expected.

6 Acknowledgements

This invention would not have been possible without the exceptional support from Harry Xiao, Arleen Liu, and Jianna Liu. I would like to thank them for contributing their time and knowledge on the blockchain technology in this project. I also acknowledge the authors of *Poor Economics: A Radical Rethinking of the Way to Fight Global Poverty*, Abhijit Banerjee and Esther Duflo, whose work inspired this invention.



Uses Service
Service Provider
Agents and Brokers
Bills insurance provider
Reimburses service provider
Consumer (Policyholder)
Finds insurance policy
Delivery Channel
Agents, brokers, contribute to markerting, client education
Validation
Claim validation
Recieves commission
Provides potential clients / policy holders
Review / validate claim
Accepts / Rejects
Contemporary Insurance Company
Accepts / Rejects
Pays premiums
Reinsurer ensures the claims of the insurer
Risk Assessment
Insurance company assess the risk of insuring
Reinsurer
Invest premiums into financial markets
Returns from markets
Risk Assessment
Insurance company assess the risk of insuring
Invest premiums into markets
Financial Markets
Returns from market

Figure 1: Contemporary Insurance Flow

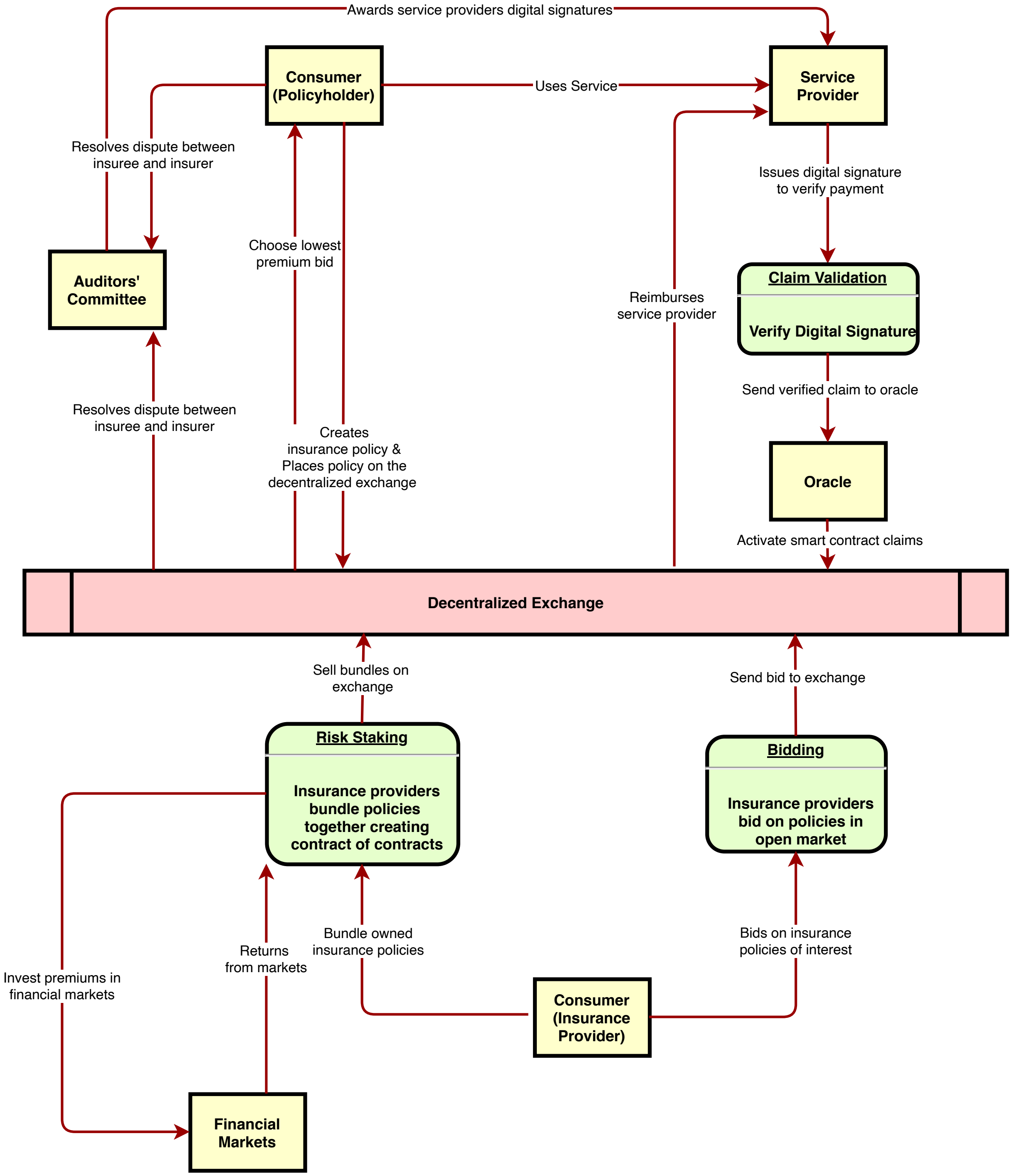

Awards service providers digital signatures
Consumer (Policyholder)
Uses Service
Service Provider
Resolves dispute between insuree and insurer
Issues digital signature to verify payment
Choose lowest premium bid
Auditors' Committee
Reimburses service provider
Claim Validation
Verify Digital Signature
Send verified claim to oracle
Resolves dispute between insuree and insurer
Creates insurance policy & Places policy on the decentralized exchange
Oracle
Activate smart contract claims
Decentralized Exchange
Sell bundles on exchange
Send bid to exchange
Risk Staking
Insurance providers bundle policies together creating contract of contracts
Bidding
Insurance providers bid on policies in open market
Invest premiums in financial markets
Returns from markets
Bundle owned insurance policies
Bids on insurance policies of interest
Consumer (Insurance Provider)
Financial Markets

Figure 2: Proposed Insurance Flow

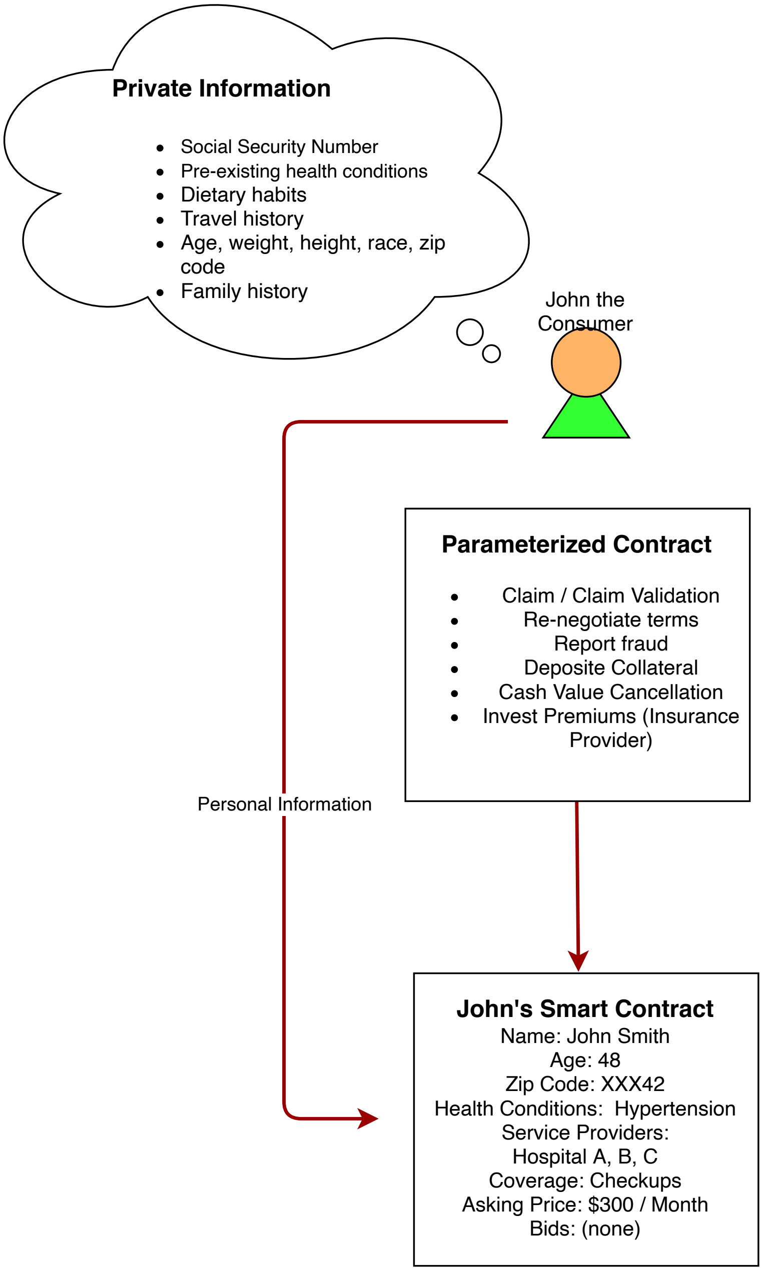


Figure 3: Creation of Temporary Smart Contract

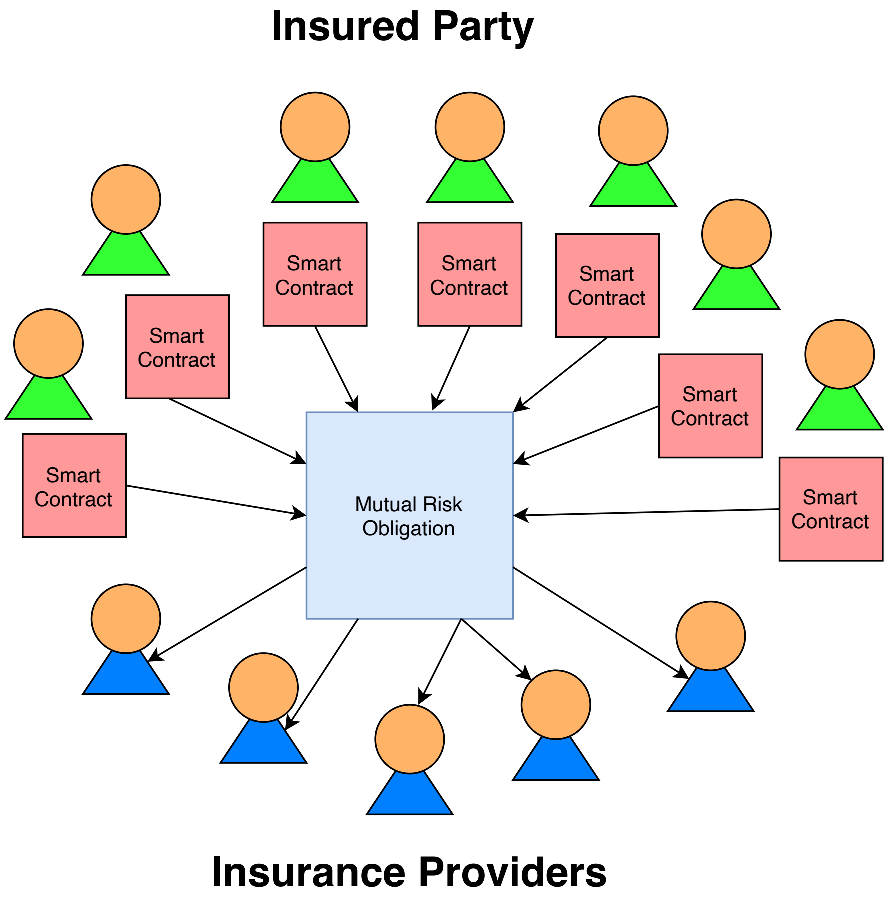


Figure 4: Mutual Risk Obligation

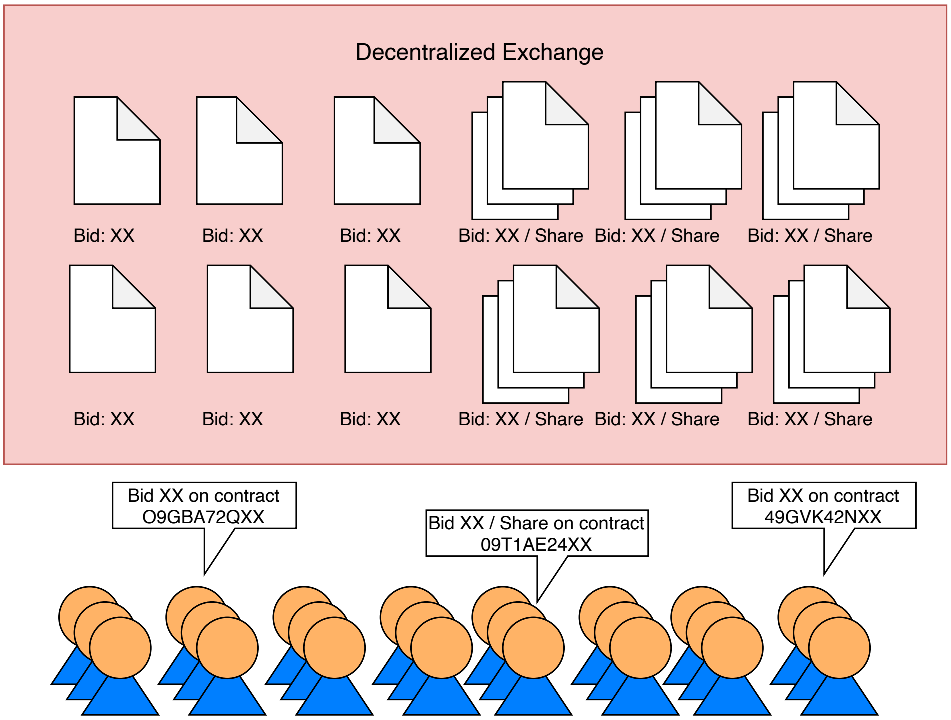


Figure 5: Bidding on Smart Contracts

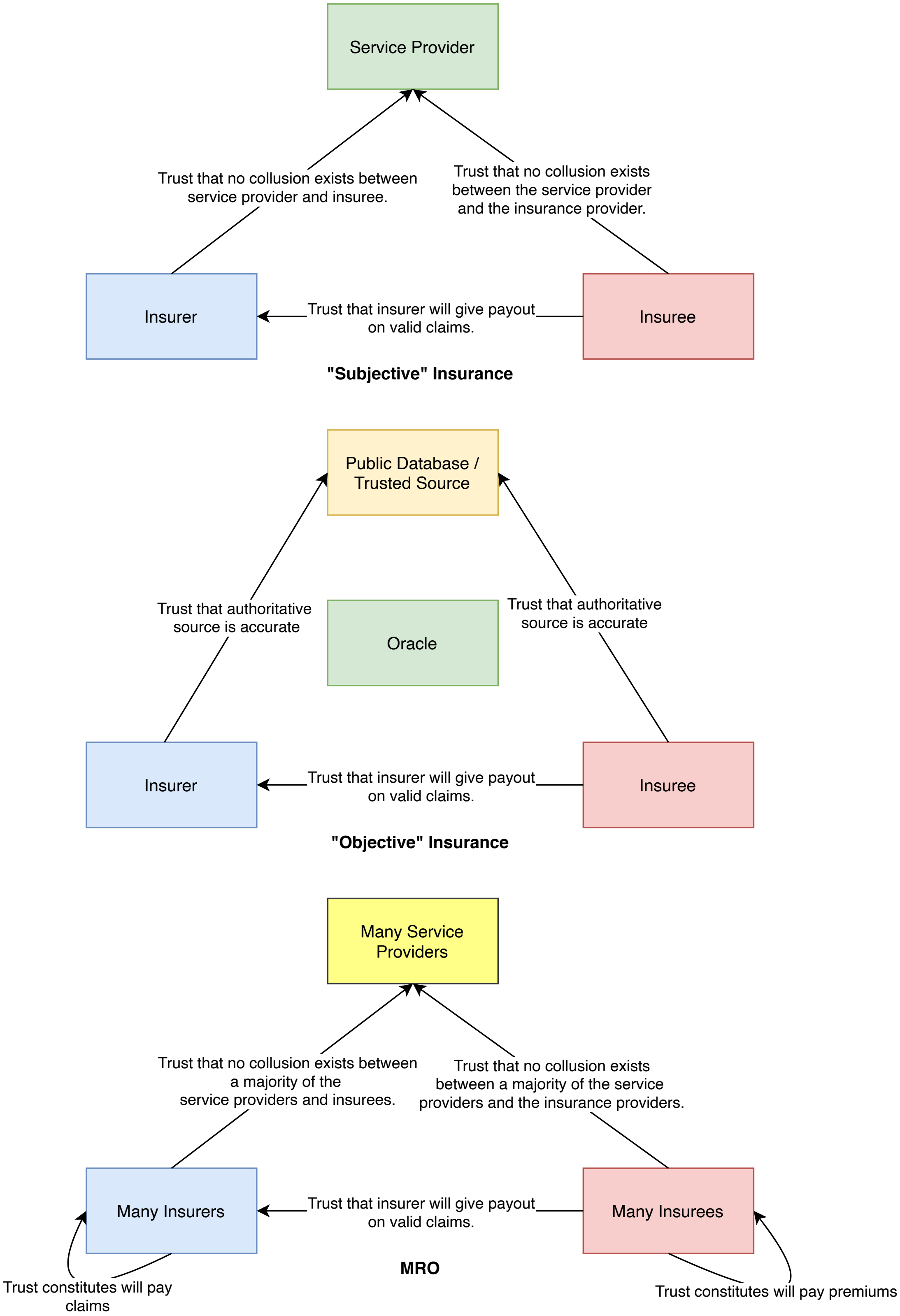

Service Provider
Trust that no collision exists between service provider and insuree.
Trust that no collusion exists between the service provider and the insurance provider.
Insurer
Trust that insurer will give payout on valid claims.
Insuree
"Subjective" Insurance
Public Database / Trusted Source
Trust that authoritative source is accurate
Oracle
Trust that authoritative source is accurate
Insurer
Trust that insurer will give payout on valid claims.
Insuree
"Objective" Insurance
Many Service Providers
Trust that no collusion exists between a majority of the service providers and insurees.
Trust that no collusion exists between a majority of the service providers and the insurance providers.
Many Insurers
Trust that insurer will give payout on valid claims.
Many Insurees
MRO
Trust constitutes will pay claims
Trust constitutes will pay premiums

Figure 6: Trust Hierarchy Between Various Stakeholders in Different Types of Insurance