ASURE: FIRST SCALABLE BLOCKCHAIN NETWORK FOR DECENTRALIZED SOCIAL SECURITY SYSTEMS

Paul Mizel, Fabian Raetz and Gamal Schmuck
Asure Foundation

October 1, 2019

https://asure.network

Abstract

Social security is an essential element in the economic and political development of societies. However, there are over 4.1 billion people worldwide without access to social security systems.[1] And on the other hand, the existing social systems have other challenges that have to be overcome for demographic reasons (e.g. birth rates 1.5 compared to the world average of 2.5) or cost reasons (administrative costs of more than 50% or even more than 100%). The Ethereum blockchain is currently only able to carry out a maximum of 1.3 million transactions per day.[2] Social security systems are based in part on several hundred million transactions per month and thus cannot be sustainably implemented using the blockchain as of today.

Blockchain-based social security systems have several advantages in comparison to conventional social security systems. They ensure a constant and much higher quality of the data used and stored through process integrity, immutability and the sustainability of the system, enabling accurate real-time analysis of those. The transparency and immutability of the transactions ensure the system's security against manipulation and corruption. By using Blockchain to remove the cumbersome and error-prone manual labor it is possible to achieve a high degree of automation, cost-efficiency, as well as easy to follow business processes.

The past developments of blockchain technology and their results show that financial transactions executed through them can be carried out securely, automatically and without intermediaries. This suggests that social security systems, as systems serving the public and using rule-based financial transactions, are a reasonable use-case for public blockchains.

The Ethereum Blockchain corresponding solutions such as Casper, and Sharding in the pipeline that will eventually solve the scalability problem on Layer 1. Even regarding the people that don't have access to any social security systems the number of transactions required for pay-ins and payouts amounts to at least the number of people involved, i.e billions of transactions on a monthly basis for the pension system alone.

The aim of this paper is to examine a Layer-2 solution for optimal scalability while maintaining all the benefits of blockchain technology regarding decentralized social security systems.

Note: asure.network is a work in progress. Active research is under way, and new versions of this paper will appear at http://asure.network For comments and suggestions, contact us at research@asure.network.

Glossary

EVM Ethereum Virtual Machine is designed to serve as a runtime environment for smart contracts based on Ethereum.

Blockchain A system in which a record of transactions are maintained across several computers that are linked in a peer-to-peer network.

Ethereum A decentralized software platform that enables SmartContracts and Distributed Applications (ÐApps).

ETH Native token of the Ethereum blockchain.

BTC Native token of the Bitcoin blockchain.

ERC20 A technical standard used for smart contracts on the Ethereum blockchain for implementing tokens.

SmartContract A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible.

Account A hash of a public key which can hold values. Hold values can only be accessed by knowing the corresponding private key.

GDPR The General Data Protection Regulation (EU) 2016/679 (”GDPR”) is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU).

PAYG a method of financing social insurance, especially old-age provision, but also health insurance and unemployment insurance. The paid-in contributions are used directly to finance the beneficiaries, ie they are paid back to them.

Contents

1 Introduction

The Asure ecosystem consists of the Asure Network, Asure Blockchain, the Asure Platform, and third-party applications.

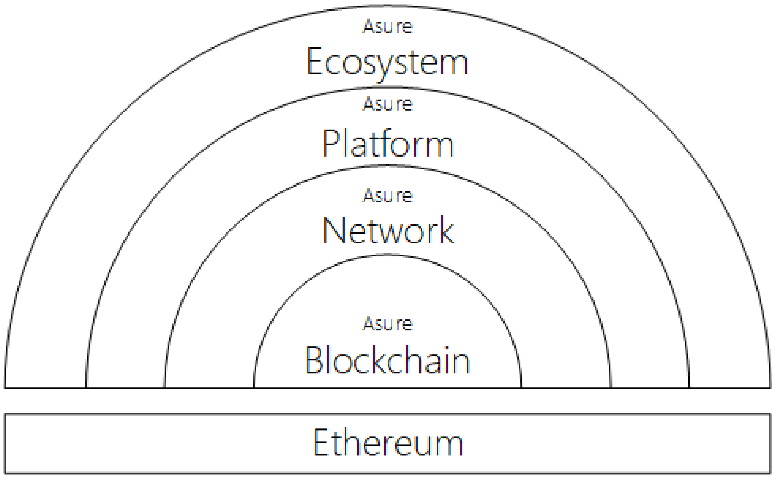

Figure 1: Asure ecosystem

The Asure network is a scalable blockchain network for decentralized social security systems. It lays the foundation for 10 billion people to have access to social security systems and achieves a great social impact where it is needed the most. [3]

As the technological base that ensures optimal performance regarding the transaction throughput while maintaining the decentralized character of the network it guarantees the required level of transparency and cost-efficiency within the system. It is implemented as many Plasma side-chains that are connected to the Asure Blockchain as well as the Ethereum blockchain or any other EVM compatible blockchain. Each side-chain is operated by several independent node providers who need to stake ASR tokens to reach consensus between them and therefore within the network. By staking ASR tokens, node providers can earn additional tokens by offering their computing power. There will be a side-chain for each social security system within the Asure network.

The Asure Blockchain contains the Asure root-chain and connected side-chains. Root-chain offers advantages in the area of security as well as interchain communication. All running Asure Blockchain nodes represent the Asure Network. The Asure Platform connects the backend infrastructure to applications which can be used by end-users or programming interfaces for developers to build applications on top of the Asure platform.

1.1 Social security systems

Social security is an insurance system in which the insured risks (such as illness, maternity, need for long-term care, accidents at work, work-related illness, unemployment, reduced earning capacity, old age and death) are covered jointly by all insured persons. Social security systems absorb many life risks, prevent extreme hardship and thus creates a social balance.

People who do not have access to social security systems are at risk of falling into poverty if they are struck by a stroke of fate such as illness, crop failure or disability. They may then have to liquidate savings, sell livestock and other means of production and send their children to work instead of the school in order to finance daily expenses. [20]

People who enjoy basic social security are more willing to invest in education and physical capital, which entail additional risks, but also the prospect of income improvements. Empirical studies suggest that the existence of social security systems, especially in the informal sector, strengthens the propensity to invest and thus promotes economic growth precisely where this best contributes to poverty reduction. [21]

It exists a broad spectrum of social security systems and they all vary in their concrete implementation. We define the functionality of the most common social security systems for the purpose of this paper as follows:

Pension

A pension system consists of a number of contributors and pensioners. The contributors pay monthly premiums which get redistributed to the current pensioners. In return, the contributors have the right to receive their pension after a certain period of time, based on the time and amount of paid premiums. In some systems, the premiums get paid by the company on behalf of the contributor which would mean a massive reduction of transactions needed. Pension payouts usually happen on a fixed date and all pensioners get paid at the same time. This makes it an ideal use case for mass payout transactions.

Healthcare

The parties in healthcare are diverse - there are insured people who pay a premium there are doctors, hospitals, pharmacies and other service providers who issue invoices. These can be offset against the system or via the insured person who submits the invoices to the system and gets the costs reimbursed. Here there are different possibilities how you can realize the processing in batches, the insured can submit the accumulated invoices at the end of the year or the doctors, hospitals, pharmacies and other service providers can also submit their collective invoices in batches.

Unemployment

Unemployment insurance is the protection against loss of work. Participants having a job pay a premium where in case of loss of work the time is bridged by the contributors to find a job again.

Social Care Insurance

The Social Care Insurance, Long-term Care Insurance or Nursing Care Insurance is a compulsory insurance to cover the risk of becoming dependent on long-term care. Social care insurance benefits are granted on the basis of "levels of need for long-term care". In the case of professional outpatient or (partly) inpatient care, the costs are covered up to a certain maximum amount (incl. nursing aids, measures to improve the living environment as well as voluntary nursing benefits). The compulsory Social Care Insurance is therefore not a full insurance. In order to achieve full coverage, it is necessary to take out a private supplementary nursing care insurance. In case of need, the insured person is entitled to assistance with nursing care as a needs-oriented supplementary social benefit.

Child And Youth Support

In Germany, Child And Youth Support covers all services and tasks of public and independent institutions for the benefit of young people and their families. Child and youth welfare is not a direct pillar of social insurance, but is mainly provided by independent institutions, which work closely with the authorities. It is mainly financed by taxpayers' money.

Invalidity insurance / Accident Insurance

The purpose of statutory accident insurance is to prevent accidents at work, occupational diseases and work-related health risks and to restore the health and professional performance of the insured persons "by all appropriate means" after the occurrence of these insured events.

1.2 Blockchain

A blockchain is a decentralized database that holds a constantly growing list of transaction records. The database is extended chronologically linear, similar to a chain to which new elements are constantly added at the bottom (hence the term "blockchain"). If a block is complete, the next one is created. Each block contains a checksum of the previous block. Satoshi Nakamoto's development of Bitcoin in 2009 is one of the blockchain implementations which shows the potential for the technology for the finance transactions. [4]

The disruptive potential of blockchain becomes increasingly apparent. After the invention of the Ethereum blockchain and Ethereum Virtual Machine (EVM), the world was given the tools necessary to build working decentralized autonomous organizations (DAO). In such a system, multiple authorities control different components and no single authority is fully trusted by all others. [5] The Blockchain technology is a perfect match to operate social security autonomously and decentralized.

2 Asure Network

The Asure network consists of the node clients in which the Asure blockchain is operated and synchronized among the individual nodes with the help of the consensus. To achieve the number of required transactions, the load must be distributed over several blockchains. One or many blockchains can be specific for a single social security system. In order to benefit from the blockchain ecosystem, and the great added value for scalability arises only when the assets can be transferred among the several blockchains. Also, specialized side-chains can benefit from the security of the root-chain and thus the assets are better protected. [6]

2.1 Requirements

The core social security and blockchain requirements in a scalable scenario are as follows:

Transaction Throughput

The Asure network must be able to scale transaction throughput through side-chains to such an extent that countries and residents can do their financial transactions within the off-chain.

Privacy

In order to protect the privacy of the users, no private data may be stored on the blockchain. If possible, transactions should not be assigned to a user. Personal data is encrypted and stored outside of the blockchain. By using the Zero-Knowledge-Proof method, the storage of personal data can be completely avoided.

In order for a blockchain-based social security to be established, it must comply with the data protection and privacy guidelines of national and international regulations such as the General Data Protection Regulation (GDPR) in the European Union. [7]

Transparency

Transparency within the Asure network is an important factor to protect social security systems against corruption and manipulation. While respecting the privacy of the users, it is important to ensure transparency of the system, in general, to enable for example real-time statistics of the overall money-flow.

Business rules for the system

Social security has many influencing factors and rules, these must be fulfilled, adapted and executed, therefore it is our requirement to be able to execute custom business rules in the side chain with EVM or EWASM.

Security

A system that organizes and stores the financial transactions of social security systems must satisfy multiple security requirements. It must be ensured that data cannot be manipulated or stolen and the system is resistant to attacks, breakdown, and other failures.

2.2 Further technologies

Poon and Buterin presented the Plasma framework in 2017 to solve the scaling problem by arranging multiple independent blockchains into a tree hierarchy. Consecutive Plasma proposals have described off-chain venues for simple transfers of fungible and non-fungible tokens. These proposals include Plasma MVP, Plasma Cash, and Plasma Debit. The Plasma framework is under active research and depending on the application and requirements the plasma implementation varies.[8] Loom and OmiseGO are one of the first who implements plasma and continues their research in this field.

Plasma was introduced very recently and is among the more promising proposed solutions to scalable computation on the blockchain. The Plasma whitepaper is very broad and doesn't have all the technical information necessary for immediate implementation. Plasma can provide scalability for Ethereum applications. It is an application-specific side-chain protocol.

Polkadot, on the other hand, was presented by Gavin Wood in 2017. The aim of the concept is to create a heterogeneous multi-chain solution that enables the connection of individually adapted side-chains with public blockchains. Polkadot allows different blockchains to exchange messages in a secure and trustworthy way.

The Raiden Network is an off-chain scaling solution with payment and state channel technology, enabling near-instant, low-fee and scalable payments. It's complementary to the Ethereum blockchain and works with any ERC20 compatible token.

2.3 Plasma

The Asure network will use the Plasma framework to create a scalable blockchain network for social security systems requirements.

To raise the limits of Layer 1 even further in order to effectively operate the social security system, Layer 2 scaling is considered to be the most efficient solution. It makes it easier to implement security in the system as it relies on Layer 1. The solution will be designed as a combination of Asure root-chain and corresponding side-chains to match social security systems needs.

Asure side-chains can be connected to smart contracts of Ethereum or any other blockchain technologies which are working with Plasma design patterns.

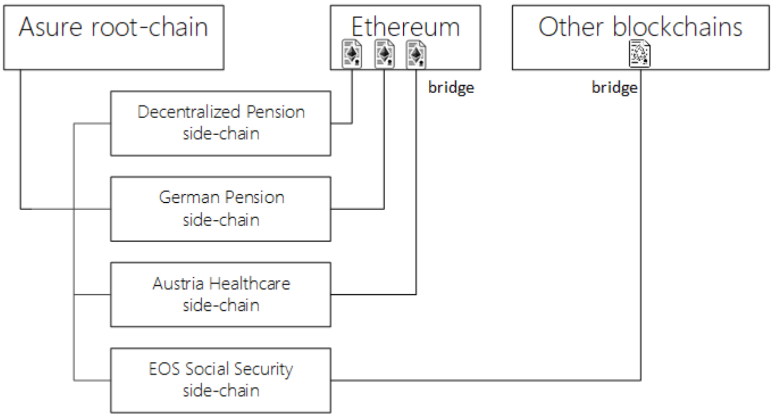
Asure root-chain
Ethereum
Other blockchains
bridge
bridge
Decentralized Pension side-chain
German Pension side-chain
Austria Healthcare side-chain
EOS Social Security side-chain

Figure 2: Asure side-chains

3 Asure Blockchain

From a technical point of view social security systems can be described as a number of rule-based (financial) transactions which are executed between a (usually) slightly changing total of different parties under the condition to maintain an equilibrium between deposited and withdrawn value over a period of time. Such a system can be implemented digitally by creating a blockchain-system, which supports smart contracts and cryptocurrencies.

Conventional social security systems currently generate up to hundreds million transactions per month, depending on the number of parties involved and the specific social security use-case.

Monthly pension premiums	= 54.445 Mio
Monthly pensions	= 25.646 Mio
Monthly pension transactions	= 80.091 Mio

Table 1: For example the German statutory pension system: [12]

In order to develop a blockchain system that can process these transactions, it is necessary to increase the achievable transaction throughput of the system and automatic batch processing within a transaction to reduce the number of total transactions to a minimum.

Both requirements can be addressed by the use of side-chains, as specified in the Plasma Framework. The Asure Blockchain functions as the scalable side-chain of the Asure Plasma implementation. It is the root-chain of the Asure Network and lays the foundation for optimal scalability regarding blockchain-based social security systems.

Assets transferred from the Ethereum Blockchain to one of the Asure side-chains, are locked up in the Asure Plasma Contract on the Ethereum Blockchain until an exit transaction on the Ethereum Blockchain is executed. According to the Plasma MVP specifications, an equivalent of this value is created through the use of the operator design pattern (Proof-Of-Authority) on the Asure Blockchain and assigned to the user.

The available assets on the Asure Blockchain can then be used for transactions within the system. Consensus between all node providers within the Asure Blockchain is reached through a proof-of-stake consensus algorithm by using an adapted version of the Tendermint consensus engine. [14] Tendermint can handle transaction volume up to 10,000 transactions per second. With the help of zones and sharding concepts, this size can be increased by a factor of 1000. This would ensure the sustainable operation of social security on blockchain. [15]

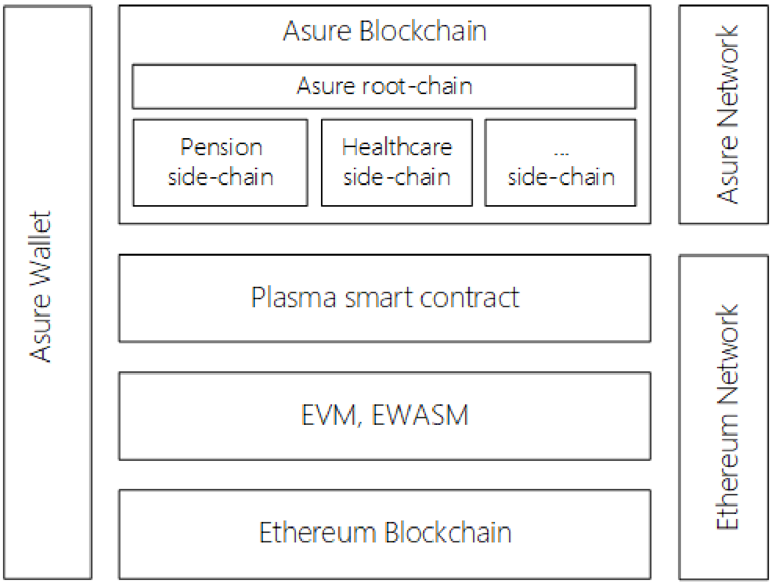

Figure 3: Asure architecture

The Asure Blockchain has several fundamentals.

3.1 Security

The Asure Blockchain includes several features that protect it against such attacks as unauthorized spending, double spending, forging assets, and tampering with the blockchain.

Each block added to the blockchain, starting with the block containing a particular transaction, is referred to as a confirmation of that transaction. Ideally, recipients and senders receiving payments should wait until at least one confirmation has been distributed across the network before assuming that the payment has been made. The more confirmations the recipient waits, the more difficult it is for an attacker to successfully reverse the transaction in a blockchain unless the attacker controls more than half of the total network performance, in which case it is called a 51% attack. This construction is not designed to prevent 51% of attacks, but rather to encourage block propagation.

3.2 Consensus algorithm

There are different versions for proof algorithms. Proof-of-work is highly criticized because of enormous power consumption.[13] Long-term acceptance and community movement is moving towards proof-of-stake where validators create the blocks and are rewarded for doing the correct job. The Asure blockchain will use a Proof-of-Stake (PoS) consensus algorithm. It will use in the first MVP implementation the Tendermint consensus engine.[14]

3.3 Privacy with (ZK-SNARKS and ZK-STARK)

Among other things, the Asure Blockchain takes into account privacy aspects that have an enormous relevance in relation to social security.

ZK-SNARKS (Zero-Knowledge Succinct Non-interactive Argument of Knowledge) offers the possibility to carry out anonymous transactions. The ZK-SNARKS are not resistant to Quantum Computing. ZK-STARK (Zero-Knowledge Scalable Transparent Argument of Knowledge) is the latest innovation aimed to achieve privacy on the blockchain with the use of fast, scalable computations and is resistant to Quantum Computing. [16]

Since Ethereum is also researching in Layer 1 in this area, it will be possible for social security transactions to remain anonymous for those insured. [17]

The state of Zero-Knowledge technologies is not yet entirely practicable, but this will change in the future.

3.4 EVM, WASM, eWASM, *WASM

EVM provides a turing-complete computation so that Ethereum can run a general program, also known as a smart contract. Plasma EVM is a new version of Plasma that can execute EVM in plasma chain, and its clients can be based on current Ethereum clients (go-ethereum, py-evm, parity). We propose state-enforceable Plasma construction to guarantee only valid state submitted to root-chain, providing a way to enter and exit account storage between two chains because each chain has identical architecture. Another benefit is that Ethereum development tools can also be used in plasma chain.

eWASM is just an Ethereum "flavored" subset of Web Assembly, which is binary instruction format. eWASM relies on instructions that are very close to real-world CPU. The performance improvements are significant and seem more secure. WebAssembly is backed by Mozilla, Google, Apple, and Microsoft, the community is also active, it's gonna be a widely used web standard.

The Ethereum Blockchain processes about 15 transactions per second (TPS), which is not sufficient for the implementation of a social security system. The improvements to Ethereum (also called Layer 1), which are currently in progress, should significantly increase the number of TPS. Among the improvements are a Proof-of-Stake (PoS) based consensus algorithm, sharding, and by the introduction of eWASM - a WebAssembly based virtual machine.

3.5 Further technologies

Parity Substrate is a high-level framework for creating cryptocurrencies and other decentralized systems using the latest research in blockchain technology.

Cosmos-SDK is a blockchain framework to allow developers to easily create custom interoperable blockchain applications within the Cosmos Network without having to recreate common blockchain functionality, thus removing the complexity of building a Tendermint ABCI application. We envision the SDK as the npm-like framework to build secure blockchain applications on top of Tendermint.

LotionJS aims to make writing new blockchains fast. It builds on top of Tendermint using the ABCI protocol. Lotion lets you write secure, scalable applications that can easily interoperate with other blockchains on the Cosmos Network.

4 Asure Platform

The Asure platform consists of components that provide the network and protocol for the use and construction of social security systems, including the Client, SDKs, tools and frontend applications. The purpose of the platform is to create an ecosystem in which social security systems can be developed, tested, simulated, managed and productively used as quickly as possible.

4.1 Client

Main client is the entry point into the Asure network, capable of running a node. Nodes are connected to each other in a peer-to-peer network and relay new information by gossip protocol. Each node keeps a complete copy of a totally ordered sequence of events in the Asure blockchain. The nodes are used to form and operate the Asure network and ensure that the transactions are included in the Asure blockchain.

4.2 Software Development Kits (SDKs)

The SDK provides standardized features on which applications can be built. Our primary goal is to simplify the development of new ecosystem solutions so that they require little to no developer support.

4.3 Tools

The tools support the creation, testing, and simulation of created solutions on the Asure network and blockchain and speed up the development process.

4.4 Frontend applications

In order to achieve user acceptance, the blockchain standard applications are provided, such as blockchain-explorer, pool, mobile-apps (Android, iOS,) with a wallet to make the experience of mobile payments on a global scale possible, as well as unlocking the full potential of mobile commerce.

5 Past Work

Asure's primary focus within the social security field is on pension insurance. As part of the ongoing research, we have ported the specific aspects of the German pension system to Ethereum blockchain. Based on both, our hands-on experience and our expertise from years of working in the insurance field, we developed the theoretical backbone of how a decentralized pension system is supposed to function as well as the proof-of-concept implementation of such a system.

5.1 Research on the blockchain technology and automation

Asure's CTO, Fabian Raetz, did a research project at the University of Applied Science and Art Dortmund in 2013 where he analyzed the emerging blockchain technologies and its possible applications. [18]

In 2014 a small team led by Paul Mizel and Fabian Raetz developed their own blockchain based currency as a proof of concept and tested different kinds of blockchain issues and economic systems (NRJ Coin). [19]

Paul Mizel has built a team in Kiev late 2015 for AI-based innovation projects "Insure Chat", "Insure Assistant" and "Insure Advisor". The applications that were built as a result were fully automated chatbots for support, claim management, and other tasks with a unique learning mechanism and connection to social platforms like Facebook, Telegram, Skype, and others.

Tech stack: IBM Watson, Microsoft Bot Framework, MS Luis, .NET.
Algorithms used: Text mining, regression analysis, SVMs, neural networks.

5.2 German Pension System

In order to demonstrate the potential of blockchain-based social security, Asure created a prototype based on the model of the German statutory pay-as-you-go pension system.

The Asure dApp will become the reference implementation for dApps using the Asure blockchain and platform.

It will feature

- a technical feasibility study of the german statutory pension system implemented on the Ethereum blockchain and the Asure protocol / platform.
- a complete wallet implementation.
- an overview and management of your insurance policies.
- an insurance store to find and buy insurance policies.

Please try out the Asure dApp which runs currently on the Ethereum Rinkiby testnet: https://dapp.asure.io

5.3 Decentralized Pension System

To demonstrate that blockchain can solve problems globally, Asure also developed a prototype of a global pension system which is fully decentralized and hence lies neither in the hands of governments nor of any insurance company.

This is an alpha-phase experiment designed to show how social security systems can be improved in the future with the help of blockchain technology.

The idea is to implement a pay-as-you-go pension system on Ethereum blockchain. Members pay their contributions in ETH and receive ERC20 tokens in return. No contributions are invested in the capital market and therefore no interest is earned. Instead, the paid-in ETHs are used directly for the payment of outstanding pension claims. How much pension is going to be paid out depends on how many pension tokens a pensioner has, i.e. how many contributions he paid into the system.

As a rule, pay-as-you-go systems only work because states introduce mandatory social security systems and, thus can guarantee a stable number of members and contribution payments. In a decentralized pension system nobody can be forced to become a member. Asure's membership creates several incentives that are intended to lead to mass acceptance.

In the decentralized pension system as well as in a classic one, whoever makes a higher contribution gets a higher pension. Pay-ins longevity plays a role as well. The longer one makes regular pay-ins the longer the pension is going to be paid out.

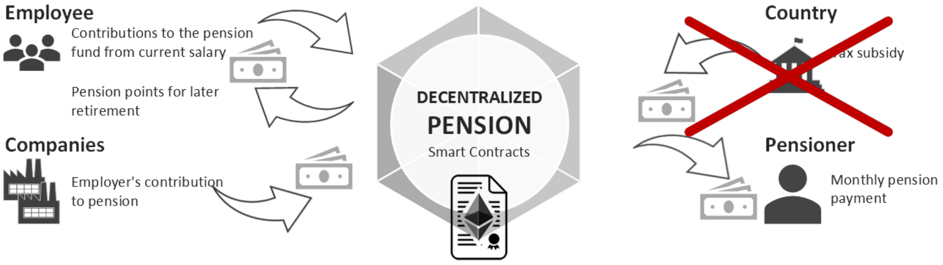
Employee
Contributions to the pension fund from current salary
Pension points for later retirement
Companies
Employer's contribution to pension
DECENTRALIZED
PENSION
Smart Contracts
Country
ax subsidy
Pensioner
Monthly pension payment

Figure 4: PAYG Model

The Asure decentralized pension dApp runs currently on the Ethereum Rinkeby testnet. It was developed during ETHBerlin hackathon and can be accessed via the following link: `https://ethberlin.asure.io`

Pension is a bet that the value I pay in is at least as great, if not greater, as the payout. The decentralized pension is based on the German pension system and has implemented a "generation contract". The young generation pays the older generation according to their possibilities and in return, the pension entitlements are tokenized, In the form of pension entitlement tokens (PET).

Incentive models were developed within the project

The system excludes the administration of age, thereby avoiding fraud and evidence. The time is divided into periods where a period is a month. Within each period deposits can be made. For each period a target price is fixed, which can shift if the median of the deposits of the previous period has a big difference to the target price.

If the maximum number of periods has been paid in, the maximum number of pension payments is also possible. Let's assume that the maximum number of periods is 480 equal 40 years. For monthly payments of 40 years, there is a claim to 40 years pension. If someone has only used the system for 2 years, the application is for 1 month only. The incentive to use the system to the maximum rewards the participants with more pension entitlement period.

$$entitlementMonths = \frac{payedMonths^2}{12 \cdot 40years} \tag{1}$$

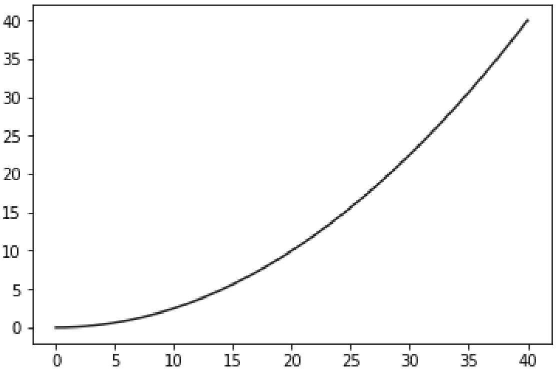

Figure 5: Decentralized pension payed vs. recive years

Since everyone can pay in different amounts in the system, the maximum payer is granted a maximum of double pension entitlement. All those who pay in more than the target price of the period will receive more PET up to a maximum of 2 per period. Maximum achievable 960 PET, this allows a later claim to twice as much in redistribution as someone who activates 480 PET.

$$DPT = \begin{cases} 1 + \frac{amount - amount_{max}}{targetPrice - amount_{max}} * DTP_{bonus} & amount \geq targetPrice \\ \frac{amount - amount_{min}}{targetPrice - amount_{min}} * DTP_{bonus} & otherwise \end{cases} \tag{2}$$

$$targetPrice - amount_{max} \neq 0 \quad and \quad targetPrice - amount_{min} \neq 0 \tag{3}$$

As a further incentive for the early adopters, a bonus was provided in the system which has a multiplicator of 1.5 and with the time logarithmically approaching 1.0 is planned to approach annually.

$$DTP_{bonus} = f(year) = 1.5 - 0.12 * log(year) \tag{4}$$

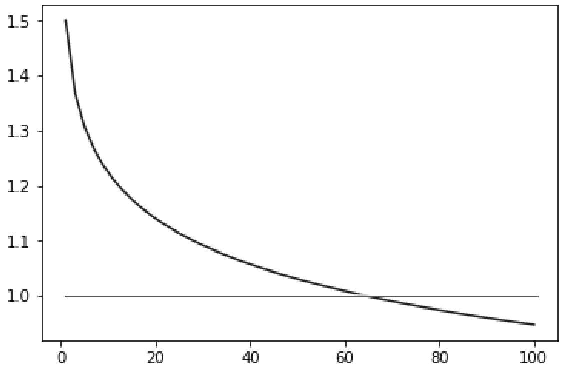

Figure 6: Decentralized pension bonus by year

If everyone leaves the system, the last participants are rewarded more, thus we guarantee that the system remains lucrative, with zero participants in the system the system is set to its initial state again.

By the limitation on maximally 2 PET or with the factor 1.5 initially 3 PET per period in the first years a utilization possibility results with several accounts into the system to pay in which the system prevents that the PETs are not transferable.

With the help of these incentives and transparent design and DAO approach, this will start as a social experiment after necessary simulations and parameter adjustments on Ethereum mainnet.

Benefits

Independent Crypto Pension has many advantages, the intergenerational contract allows the inflation security. It is autonomous and decentralized according to the idea of the DAO. There is no intermediary. The privacy is secured because no personal data is necessary to participate in the system. It is completely transparent as all transactions are on the blockchain and it is also open source.

Read more

We summarized our ideas on how a redistribution based peer-to-peer pension system might look and share our results with the broader community.
Depot Paper: `https://www.asure.network/asure.depot.en.pdf`

6 Future Work

This work presents a cohesive path toward the construction of the Asure network; however, we also consider this work to be a starting point for future research on decentralized social security systems. In this section, we identify and populate two categories of future work. This includes work that has been completed and merely awaits description and publication and open questions for improving the current protocols.

6.1 On-going Work

The following topics represent ongoing work.

- Plasma MVP implementation.
- Mobile Application (Android, iOS)
- Decentralized social security system research.
- Asure-in-Ethereum interface contracts and protocols.
- A full implementable Asure protocol specification.

6.2 Open Questions

There are still some areas for improvement that can positively affect the performance of the network. They can be addressed later on after collecting enough statistic upon which can be decided the importance and the necessity of making changes:

- A better solution for mass enter and exit strategies.
- A secure solution for the data unavailability issue.
- A more practical application of SNARK/STARK.
- A better strategies for faster implementations of social security systems and new economic models.
- A better primitive for the Proof-of-Stake Prove function, which is publicly-variable and transparent.

Since social security is only a specialized form of insurance it is obvious to also support decentralized insurances on the platform and that it is a good match to expand this platform for the market. The Asure ecosystem consists of the Asure network, the Asure protocol, the Asure platform is powered by potential third-party applications in the field of social security and the insurance environment. The acceptance of the ecosystem will grow steadily due to the resulting network effects and synergy effects.

7 Organisation

The Asure Foundation is a non-profit organization which is based on three main pillars: innovation, collaboration and research with a community of members engaged in research and development for newly developed solutions created on the Asure network, blockchain, and platform to design blockchain solutions with social security and insurance systems in a DAO fashion.

The foundation includes technology researchers as well as insurance experts. The Asure Foundation is an integral component of our work, that lets us coordinate interactions in different parts of the ecosystem.

8 Acknowledgements

This work is the cumulative effort of multiple individuals within the Asure Foundation team, and would not have been possible without the help, comments, and review of the collaborators and advisors of Asure Foundation. We also thank all of our collaborators and advisor for useful conversations; in particular Andrey Kuchaev, Alexander Böhner, Dirk Mattern, Dennis Rittinghof, Michael Lurz, Emanuel Kuceradis and Prof. Dr. Hirsch.

Conclusion

Although finding functioning scaling solutions regarding blockchain-systems is a wide topic and needs a lot of more research in general, the evaluations in this paper state that efficient solutions to improve or even replace existing systems can be built by using blockchain while maintaining financial and socio-cultural benefits. Plasma has great potential to work as the technological scaling base specifically for social security systems based on blockchain. Taking into consideration several difficulties like data unavailability, other issues, and the large community working on this issues, it's a stony path, but also a feasible one.

We at Asure believe that the future of social security and insurance will be defined by blockchain technologies in a decentralized way, which creates a whole new experience geared for the digital world. It can only be achieved by using a decentralized blockchain platform as the basis for creating a network, blockchain, platform, and protocol for any kinds of risks in the world.

The concept of implementing social security via the blockchain is unique and offers an enormous potential to improve human life worldwide. The promotion of social security on Blockchain would bring more trust, satisfaction, freedom and world peace. Asure is conceptually open, and we believe that it is very well suited to serve as a fundamental platform for a very large number of social security solutions in the coming years.

With our token sale, we want a wide range of people to participate in this long-term journey and create a success story by changing how social security works in our new digital age. Be part of this journey, and join our Token Generation Event - we are looking forward to welcoming you aboard!

Website	`https://asure.network`
Medium:	`https://medium.com/AsureNetwork`
Twitter:	`https://twitter.com/AsureNetwork`
Telegram channel:	`https://t.me/AsureNetwork`
Facebook:	`https://fb.me/AsureNetwork`

List of Tables

List of Figures

References

[1] World social protection report 2017-2019, *Universal social protection to achieve the sustainable development goals*, International Labour Office, Geneva, 2nd edition, 2017.

[2] Etherscan, *Ethereum Transaction Chart*, `https://etherscan.io/chart/tx`, 2017.

[3] Worldometers, *World Population Forecast (2020-2050)*, `http://www.worldometers.info/world-population/`, 2017.

[4] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, `https://bitcoin.org/bitcoin.pdf`, 2009.

[5] Carmela Troncoso, Marios Isaakidis,George Danezis, Harry Halpin, *Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments, In Proceedings on Privacy Enhancing Technologies*, De Gruyter Open, volume 2017, 2017.

[6] David Knott, *Construction of a Plasma Chain 0x1*, `https://blog.omisego.network/construction-of-a-plasma-chain-0x1-614f6ebd1612`, 2017.

[7] GDPR Info, *General Data Protection Regulation*, `https://gdpr-info.eu/`, 2018.

[8] Joseph Poon and Vitalik Buterin, *Plasma: Scalable Autonomous Smart Contracts*, `https://plasma.io/`, 2017.

[9] Minimal Viable Plasma, `https://ethresear.ch/t/minimal-viable-plasma/426`, 2017.

[10] Plasma Cash, `https://ethresear.ch/t/plasma-cash-plasma-with-much-less-per-user-data-checking/1298`, 2017.

[11] Ethereum, `https://ethereum.org`, 2014.

[12] Deutsche Rentenversicherung, *Wichtige Eckzahlen*, `https://www.deutsche-rentenversicherung.de/Allgemein/de/Navigation/6_Wir_ueber_uns/02_Fakten_und_Zahlen/03_statistiken/wichtige_eckzahlen_node.html`, 2016.

[13] Andrew Tayo, *Proof of work, or proof of waste?*, https://hackernoon.com/proof-of-work-or-proof-of-waste-9c1710b7f025, 2017.

[14] Jae Kwon, *Tendermint: Consensus without Mining*, https://tendermint.com/static/docs/tendermint.pdf, 2014.

[15] Zach, *Tendermint: Benchmarks*, https://github.com/tendermint/tendermint/wiki/Benchmarks, 2018.

[16] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, Michael Riabzev, *Scalable, transparent, and post-quantum secure computational integrity*, https://eprint.iacr.org/2018/046.pdf, 2018.

[17] Christian Reitwiessner, *zkSNARKs in a nutshell*, http://chriseth.github.io/notes/articles/zksnarks/zksnarks.pdf, 2016.

[18] Fabian Raetz, *Aufbau und Funktionsweise des Bitcoin-Protokolls*, 2014.

[19] NRJ Coin Project, *NRJ Coin Project*, https://github.com/nrjcoin-project, 2014.

[20] European Report on Development (ERD): Deutsches Institut für Entwicklungspolitik, https://www.die-gdi.de/erd/, 2018.

[21] Health as Human Capital: Theory and Implications A New Management Paradigm, HCMS Group, http://www.hcmsgroup.com/wp-content/uploads/2012/05/WP01-HHC-Theory-and-Implications-2012-01-161.pdf, 2012.

[22] etherscan.io: gaslimit chart, https://etherscan.io/chart/gaslimit, 2012.

Made with ♡ in Germany