FreeTrust Project Current State

051115aWW

FreeTrust folder - Slide Deck - LightningTalk Template - Domain Names - Synereo - eris - Identifi - Stellar - Factom - Ethereum - Synereo Video - Synereo - onename - CoinSource - consensus algorithm - Stellar Consensus Protocol PDF - Ethereum Talk - Counterparty - : The Blockchain - Early discussion - blockchain passport - Keybase - NSTIC Privacy Pilot - proposal.

To participate comment (select phrase and click the comment bubble), edit in suggested changes here directly and get an invitation to freetrust.slack.com at FreeTrust.net.


Identifi


Free Trust at FreeTrust.org: The Privacy Revolution

Trusted Identity, Privacy, and Safety in Cyberspace

FreeTrust represents a vision of an inevitable future of cyberspace giving users the privacy they deserve while enabling the development of personal webs of trust integrated anonymously with global identity ecosystems by trustworthy consensus mechanisms. FreeTrust proposes a pilot integrating existing open source platforms, employing existing standards to provide individuals a private information resource service obeyed in their trusted networks. The pilot will demonstrate local grassroots trust which can build into organizational trust. It will enable trust in personal, organizational and global blockchains, in addition to traditional sources of trusted identity and authorizations. The individual, as his own identity provider, may be trusted if he has been reliable. It will demonstrate user managed identity, presence, security, privacy and uniqueness and the related authorizations in a proven private distributed social networking environment. Privacy is essential such that the individual user controls what information is true and does not misrepresent him by his own judgement and exposure that may be limited to who needs to know it. Enabling freedom of trust is important as trust enables collaboration, which enables innovation, which enables enterprise, which enables the evolution of a better quality of life.

What if:

- You could prove your identity once instead of to each site you visit.
- You could develop a trustworthy anonymous identity online that is good everywhere for all your persona.

- You could manage your identity and other personal information resources yourself with proven privacy.
- Instead of using insecure email, chat and social networks everyone could use FreeTrust social networking with proven security and privacy.
- Instead of a “To:” list you have a "who needs to know?" and "who's allowed to see?"
- In this manner you seed new FreeTrust identities from whom permission will be requested if you want to share each others information resources. They then become FreeTrust users.

Strong anonymous translucent identity with trusted interaction is a goal of FreeTrust, both trustworthy to be safe and opaque to protect personal privacy.

FreeTrust:
Voluntary Trusted Identities, Privacy and Safety in Cyberspace
DRAFT 0.5

Identity is the new money
FreeTrust - Decentralized Identity
The Identity Ecosystem Current State
A New Paradigm
Blockchain distributed databases
The Nature of Trust
- Trust as predictability
- Trust as fair value exchange
- Trust as Delayed Reciprocity
- Trust as exposing vulnerabilities

- Trust managed in FreeTrust
  - Trust granted as a delegation of authority
  - Trust as corroboration of a claim
- The Privacy Trust Factors metrics quantified in FreeTrust
  - Identity
  - Presence
  - Security
  - Privacy
  - Uniqueness
  - Other Trust Domains
- FreeTrust Trustworthiness
- Crowdsourced Trust Factors within Webs of Trust
  - Individual Quantized Trust Rating and Ranking
  - Group Trust Rating and Ranking
  - Limited and Revocable Trust
- Trust Consensus “mining”
- Social Networking Component
- Economic model
- Architecture
  - Synereo Dapp component
    - Identity Ecosystem Integration
    - Social Contracts
    - Personal Information Resources Services
    - User Agent
    - Collaboration Agents
  - Identifi Dapp component
  - Eris Dapp component
  - MrE Inference Engine
- Operational Pilots
  - ProvenSecure Solutions Inc. (PSSI)
  - Clarkson Pilot
  - Clarkson University Pilot
  - Altrucoin
  - WikiWorld
- links
  - Identifi

Identity is the new money

The internet has been transforming society by empowering individual expression and connecting us in unprecedented ways where the sum of human experience can be reached at one's fingertips empowered by intelligent systems that are becoming slaves of humanity. While

old institutions are fading and business has largely become an accounting of eyeballs, the transformations continue in each phase of the internet, from websites and email to the development of user communities connected by social networks capitalizing on the personal information of the participants. Identity has become the new money where the valuation of an enterprise has become a multiple of the size of the user community.

There are numerous issues today that will lead us to the next phase of the internet. Identities on the internet are generally very weak. Where there is any assurance at all it is usually just that a confirmation email was received by the claimed email address. There is no assurance it was received by an actual person rather than some mechanized autoresponder. Personal information is exposed to more and more systems directly and by linking accounts sharing contact lists. Users are forced to extend their trust to whatever services their contacts use. The list of services one must trust grows continually; PayPal, Facebook, GitHub, LinkedIn, and so on.. Due to exposure, it can be expected that personal information will be used in a manner that ultimately violates the user's trust. The new internet must be trustworthy. There is a recognized need to both put people back in control of their personal information and to have stronger assurance of the identity of people, organizations, services and devices that are part of an online interaction. FreeTrust applies a next generation architecture to eliminate the imposition of extending trust that has not been earned on the individual. At the same time, it empowers people, organizations, services and devices with a strong identity having both greater value and safety in the coming phase of the internet. FreeTrust is an architecture and an idea whose time has come.

FreeTrust - Decentralized Identity

FreeTrust provides a user interface to manage personal information resources in the identity ecosystem (UMA, XACML, OpenID, SCIM, LDAP, etc.). It is built on blockchain identities and a Decentralized Distributed social networking platform (Synereo) that enables user trusted identity, presence, security and privacy for the individual with a consensus mechanism in Cyberspace that grows collaborative trust organically. As trust is extended to others it grows into trust networks, organizations, federations and global identity ecosystem connected globally using blockchain technology. Users can develop trustworthy identities without having to trust any authority. Then trust built among individuals can become trusted in communities and ultimately trusted by governments in national identity ecosystems. It promotes global assurance that an entity participating in an interaction is a trusted human, organizations, service, or device, revealing information about the entity only when authorized on a need to know bases. FreeTrust puts the user in total control of their personal information and allows them to build their own trust networks to become an equal participant in the identity ecosystem. It gives everyone the freedom to not trust the public, governments, corporations, or anyone with private information they do not need to know.

FreeTrust is a distributed application implementing an interface to a mashup and selection of APIs of existing open source distributed applications, installable by the user, which are already available to provide most of the underlying functionality.

The Identity Ecosystem Current State

The emerging identity ecosystem in the US supports users' identity OpenId persona to be authenticated only once for access to most all systems used. You will be able to control access to your bank account and your home security system all using the identity provider of your choice, the one you trust with your personal information. This provides you some assurance no one else is acting as you. User managed authorization (UMA) standards allow you to easily give your brother access to your bank account, or people on a friends list access permission of a file you own. The National Institute of Standards (NIST) boasts that you can even be your own identity provider, running your own IdP service and be part of the national identity ecosystem yourself.

But, who will trust you to be your own identity provider? Unless some trusted provider trusts you, your identity will be worthless despite the fact that you are the best source for most identity factors about yourself. The goal of FreeTrust is to construct a mechanism to connect bottom up trust with top down trust, putting the user in control of personal information while making systems more trustworthy. Insuring trust from the bottom up is more effective than from the top down. For bottom up trust no one can be forced to trust anything, FreeTrust gives the individual freedom to trust only what they actually trust. This gives them a feeling of safety.

Not everyone trusts Google, Microsoft or GitHub individually. Some think those systems have already been compromised or inevitably will be compromised. They do not trust those organizations to handle their information in their best interest. They object to giving personal information to every website they go to in order to use it. Some view being forced to use GitHub or any site they must trust with their information as a potentially dangerous invasion of their privacy and threat to their personal information, intellectual property and work product. Some refuse to collaborate using any big sites.

A New Paradigm

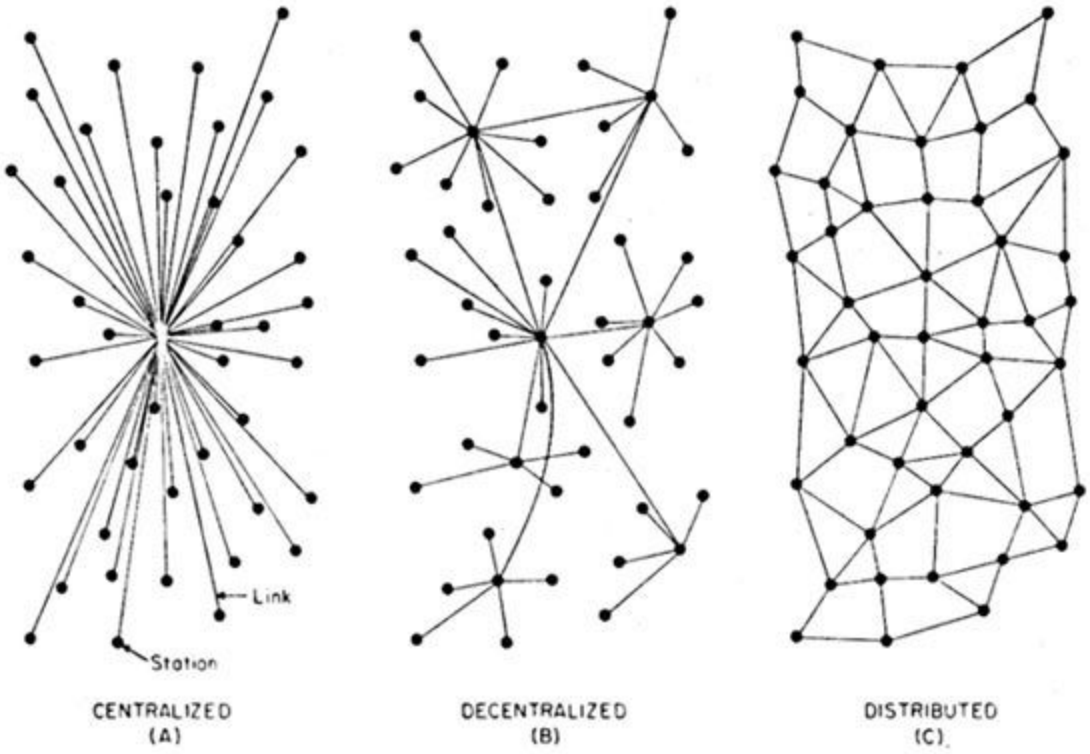
The new architecture and business model sweeping the internet is the trustworthy *Decentralized Application* (Dapp) that is open source, runs everywhere, has no central authority, runs autonomously and has built-in scalable economics. more...

Dapps are different in that they are owned by no one and run all over the network. If properly developed and deployed, you would need to hack into more than half of the systems on the network to break the security. It is an algorithm and API for achieving consensus among peers leading to a global consensus of a record of transactions without any centralized system involved.

Distributing the application with end to end encryption means the network need not be exposed to any private information and need not be trusted. There is no central company or system that might be corrupted or targeted to harvest personal information not shared publicly.

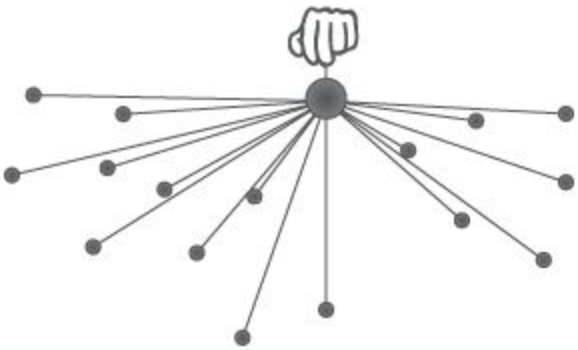
It is suggested that the Dapp model will replace centralized services like Facebook, Google, GitHub, etc. in time and become dominant in the next phase of the internet. FreeTrust aims to accelerate adoption of Dapp's by providing a trustworthy framework for decentralized trust and consensus supporting a mashup of Dapp's and their currencies It is a realization of the "Web of Trust". It will link user authorizations between national identity ecosystems and blockchain identity and extend the ability to set permissions on posts, bank account and thermostat in a distributed social networking environment with proven levels of security and privacy. FreeTrust will give users complete freedom to choose what they trust maintaining privacy with trusted identity and trusted security. FreeTrust takes the potential of trustworthy transactions, as in Stellar and eris machine consensus and applies it to human consensus. FreeTrust jumps onto the Stellar bandwagon and takes it beyond trustworthy transactions to trustworthy identity, presence, security and privacy.

Arguably, "trusted computing" on the web is a key tenet of the new crypto-driven paradigm. Cryptocurrency 2.0 has become "the digital consensus space".

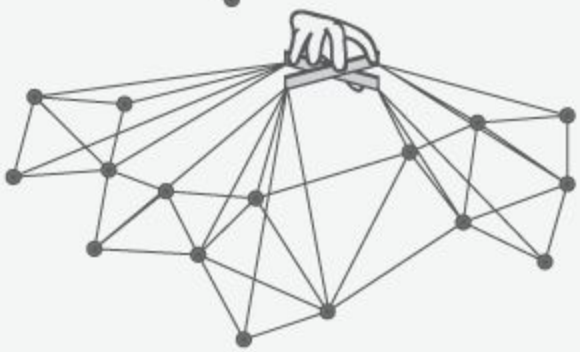


Source: On Distributed Communications Networks, Paul Baran, 1962

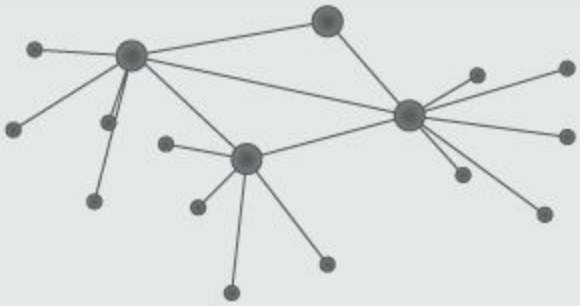
xhttps://t.co/a2wf2Xf9Ym



Centralized



Distributed



Decentralized

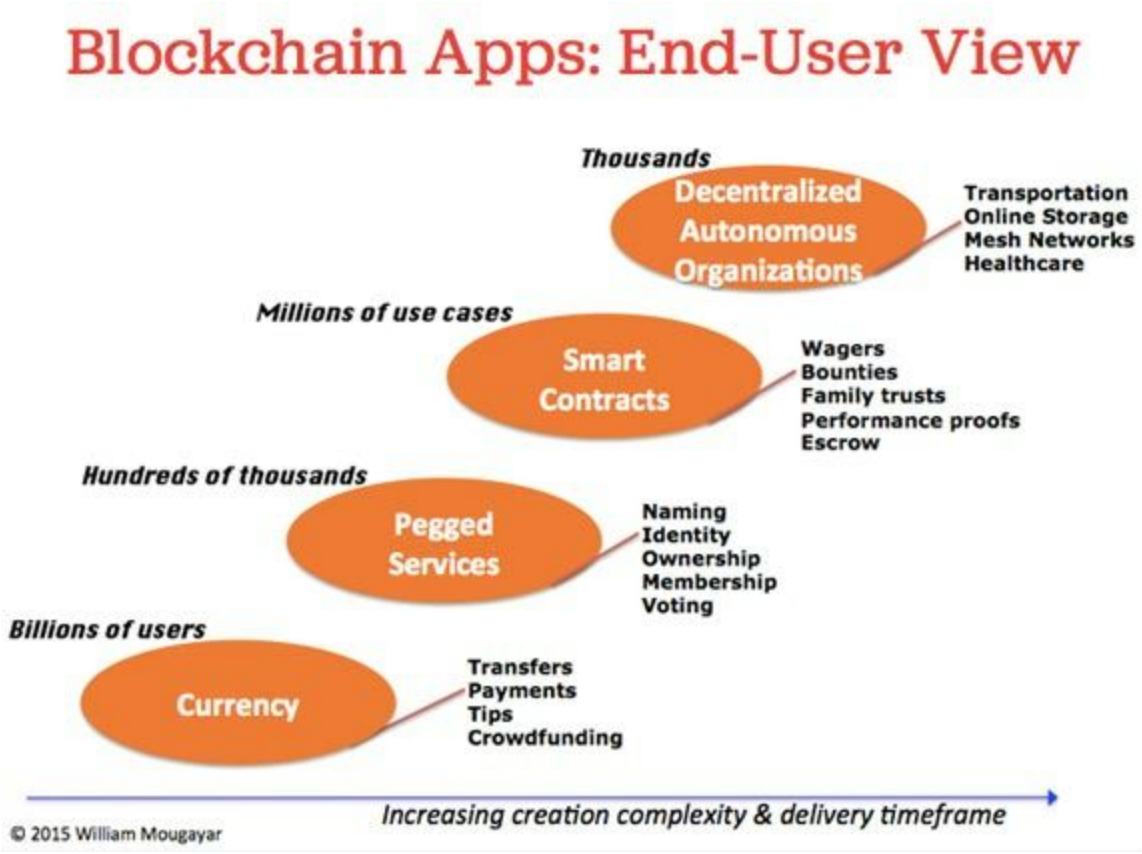
Blockchain distributed databases

A blockchain is a distributed ledger of transactions and other multi party processes that can not be altered in perpetuity. It is the secret sauce that ensures the reliability of bitcoin and other blockchains. But FreeTrust does not demand trust of even the Bitcoin blockchain. Blockchains are distributed across the network but are still a singular entity that is subject to attack by unknown threats. And thousands of blockchains have been created which might earn trust. Global consensus is often unnecessary for trusted consensus to emerge in a trust network of individuals or organizations. Tools like Eris make it trivial to instantiate a new blockchain with whatever parameters or smart contracts imposed on it which is automatically replicated across the network. Having millions of blockchains corroborating one another eliminates a single point of attack while enabling the evolution of blockchain technology.

FreeTrust participant personas claim a unique global OpenID Connect user ID which is registered on multiple blockchains. The blockchains insure that no one else has the exact same identifier and register a key such that nobody else can claim that identity. Participants vouch for each other's trust factors peer to peer Trusted notaries can accumulate proofs in the form of corroborations scored relatively according to trust in the corroborators. In this manner an entity can become a trusted identity peer to peer, in trust circles, in trust networks, by organization and by government.

Strong identity is a missing link in the BitCoin distributed application world. As David Birch points out in his work of the same name: "Identity is the New Money". FreeTrust capitalizes on identity in a manner that encourages trustworthiness and fairness by rewarding trustworthy behaviors which create value and discouraging behaviors which destroy value. It does this both locally within local trust networks and by global consensus. It facilitates diversification in acting locally in trust networks while promoting thinking globally and achieving global consensus. By extending trust relations to others, they become part of the trust network and the network grows organically.

Source: Courtesy of William Mougayar



The Nature of Trust

Trust is an expectation based on incomplete information. Our expectations may not be reasonable. We Trust those who we Trust to share their Trust of others, thus developing a Trust;Consensus. This may only be within a trust network or organization or government and ultimately global trust. FreeTrust allows the freedom to not have expectations of others which has not been earned.

Trust as predictability

“Trust means being able to predict what other people will do and what situations will occur. If we can surround ourselves with people we trust, then we can create a safe present and an even better future.”

Trust as fair value exchange

“Trust means making an exchange with someone when you do not have full knowledge about them, their intent, and the things they are offering to you.”

Trust as Delayed Reciprocity

“Trust means giving something now with an expectation that it will be repaid, possibly in some unspecified way at some unspecified time in the future.”

Trust as exposing vulnerabilities

“Trust means enabling other people to take advantage of your vulnerabilities—but expecting that they will not do this.”

Trust managed in FreeTrust

Trust granted as a delegation of authority

This includes permissions given to others to conditionally access or expose the user’s personal information resources including personal identifying information (PII). It consists of a social contract associated with access to an entity internal or external to the networking environment.

Trust as corroboration of a claim

Corroboration of claims about another individual increases their relative trust score commensurate with the trust score of the corroborator. Providing trustworthy corroborations also enhances the trust score of the corroborator.

The Privacy Trust Factors metrics quantified in FreeTrust

Freetrust quantifies peer to peer trust factors developing consensus within trust networks, organizations and federations with the aim of developing global trust.

Identity

A strong trusted **identity** has many long lived claims regarding an entity corroborated by trusted 3rd parties. Entities possessing identity include people, organizations, devices and services.

Presence

Trusted **presence** means that the parties in an interaction have provided trusted authentication factors giving assurance identities are actually present, and are not imposters. Entities are each authenticated to one another to enable an interaction

Security

Trusted **security** means there is corroboration that their systems are protected, resilient and not compromised and thus unlikely to expose personal information.

Privacy

Trusted **privacy** means assurance that no more information than is voluntarily and explicitly authorized will be shared with 3rd parties in a manner and for purposes explicitly authorized.

Uniqueness

Preventing sybil attacks or double voting with anonymity is one aim of FreeTrust. FreeTrust builds on and improves existing P2P Web of Trust mechanisms. Besides verifiable identity factors Identity scores include a uniqueness metric.

A person may have many persona for which separate identities might be established. A user may not trust the system enough to associate those identities or has chosen to try to fool the system. This cannot be completely prevented either in the outside world or online. Very strong biometrics which can be searched against existing identities can help if the same biometrics are used for multiple persona. In FreeTrust it would be difficult to get independent strong identity for multiple persona and sharing factors between two persona could easily be discovered, one of the risks accounted for in the domain model of an identity is that it is a duplicate for which we could determine a probability based on overlapping similar factors and disjoint missing corroborated factors. To prevent discovery of pseudonyms by testing arbitrary sets for uniqueness only the user themselves can add themselves to a unique set and must meet a required uniqueness score for the set to get added.

Given that a unique individual can be determined, anonymity can be achieved by the assignment of a random anonymous id or crypto-token for an identity, but if the same anonymous id is used over and over for different purposes or ever exposed to a 3rd party it becomes useless This can be mitigated by assigning a unique random id for each independent usage. In this manner FreeTrust provides a mechanism facilitating trustworthy anonymous unique identity. It is also useful, for example, in anonymous voting. Each election would have a separate identifier which could be hashed with the userid to create a unique random identifier for that user for that election alone, such that votes per person may be restricted in a safe manner. Blockchain technology with strong identity and presence can prevent double voting or counterfeiting of ballots, currency, tickets, coupons etc..

Other Trust Domains

While the focus of FreeTrust is to promote safe private interaction among strong identities trust factors are not restricted to that domain. Other trust aspects defined by the user or organization may be quantified such as:

- honesty
- fair business practices
- expertise in a specific area
- personability

Accounting for these other trust factors at the federation and global level is outside the scope of this pilot. The pilot evaluation will simply report usage of other trust factors by the pilot groups. Identity, presence, security, privacy and uniqueness trust factors are prerequisite to a trustworthy interaction and thus other trust factors

---

FreeTrust Trustworthiness

Trustworthy permissions automatically allow one to share only what is allowed by agreement of the owner of the information resource. Trustworthy privacy would help one share information only on a need to know bases where there is risk. Trustworthy security would make the internet a safe place and reliable utility. Its strong identity and would assure users that they are dealing with real people not robots even if they are anonymous, trustworthy claims about them can be verified. A user is assured that a claimed identity belongs to the person or entity both by his/her criteria and those of the person or entity. Strong presence factors insure nobody can act as the user without his/her consent. Users can feel safe since there is no mandate about who or what they have to trust and can use what they trust. They might decide for themselves or use what is trusted by those they trust freeing them of complex decisions defered to the wisdom of trusted crowds.

Enabling trust is important as trust enables collaboration, which enables innovation, which enables enterprise, and enterprise enables a better quality of life to evolve.

Crowdsourced Trust Factors within Webs of Trust

Individual Quantized Trust Rating and Ranking

In has been shown that it is sufficient in the security context for individuals to rate risk on a simple scale: This is because humans are bad at making finer rate judgements consistent with their rankings and when risk factors are combined the result is not sensitive to small variations in aspects of individual factors.

1. no judgement
2. low trust, high risk. (0-.33)
3. medium trust, medium risk (.33-.67)
4. high trust, low risk (.67-1.0)

In the case of no judgement. judgement is deferred to objective criteria, trust networks and communities by rank order of personal trust. Low medium and high trust groups may each be ranked ordered both personally and by promotion or demotion according to feedback producing an ordering that can be used in approximating a consistent linear trust scale given sufficient list size.

Group Trust Rating and Ranking

The security realm is too complex for any individual to be competent in all aspect of it. Freetrust facilitates collaboration on specified trust transitivity in personal trust networks. From individual ratings and ordering group ratings and rankings are developed. averages of individual ratings (excluding no judgements) crowdsourced higher precision rating and thus ranking of trust factors within trust networks. The precedence is first personal trust is considered, then Web of Trust, organizational, federation and finally global trust consensus when possible.

Limited and Revocable Trust

“Fool me once, shame on you. Fool me twice, shame on ME.”

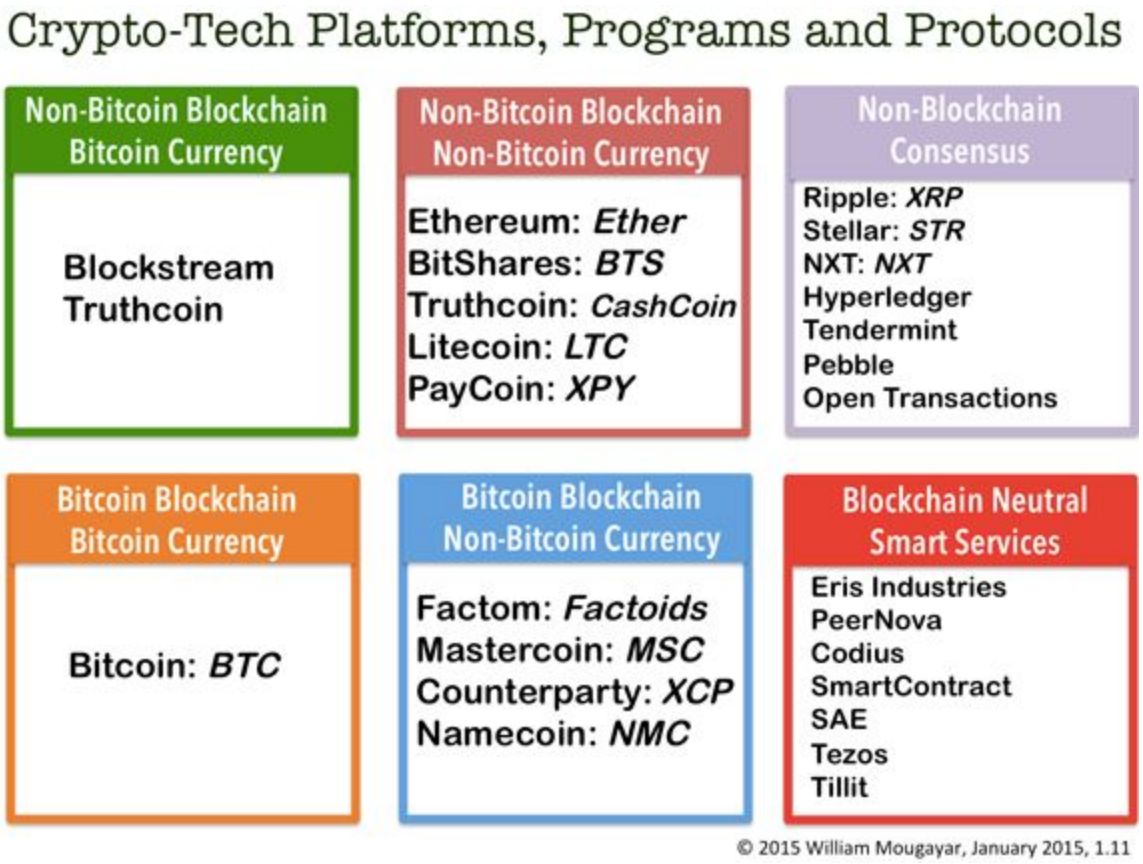
Trust can change in a blink of the eye. Users ought not be victim of their former trusts. Revocable trust provides a strong incentive for trustworthy behaviour. Providing a URI into a user's personal information server acting as a ticket subject to the permissions granted means that the receiver need not store the actual personal information but only the URI. This frees the receiver from the responsibility and liability associated with storing the information while allowing the owner to revoke permissions at any time.

Limitations may be subject to any social contract and may include access count, time period, location and usage restrictions.

Trust Consensus “mining”

FreeTrust capitalizes on trust factor consensus without depending on the bitcoin blockchain for global consensus. Instead it employs techniques like proven safe mathematically Federated Byzantine Agreement, “consensus algorithm” developed by Dr. David Mazières of Stanford University for the Stellar Development Foundation to provide an immutable trustworthy global consensus in a Web of Trust ultimately enabling global decisions. Governance of FreeTrust is according to such consensus. FreeTrust applies Maximum relative Entropy (MrE) analysis to disputes leading to better choices. Consensus resolution is the electricity of the network rather than less desirable hashing to get the same effect. No single blockchain is trusted. A single hash of many agreements is periodically hashed and stored on other blockchains to immortalize the consensus of the hour for simple immutable validation by at least 2 of 3 blockchains at any time in the future should there be a dispute due to system corruption such that even a few trustworthy nodes may carry on isolating the corrupted blockchain. FreeTrust is blockchain agnostic and includes the ability for users and groups to create their own blockchain as a record they trust replicated on the network. These may be used for any kind of accounting with application is creating electronic tickets, coupons, elections, and local currencies. The eris platform is designed to support millions of blockchains each having a configurable smart contract programmed consensus mining mechanism..

Trust networks from different perspectives must be proven to be consistent. Proof of work consists of reporting on agreements and disagreements discovered but this accounting is reported and verified with anonymity. Trust factors including strong identity, presence, privacy and security are capitalized on in FreeTrust such that the system maintains scalable economics promoting assurance of trustworthiness. Anonymous identity is supported having verifiable identity and presence factors with penalties against personas of a person double voting and lying by playing both sides of the fence. Trust “miners” are rewarded with fees paid to the network in Privacy coin. The users node in FreeTrust both earns fees for the network's use of it and pays fees for the use of the network such that they network serves everyone with scalable economics. FreeTrust aims to be blockchain agnostic.



Social Networking Component

FreeTrust unites the world of social networking and user managed authorization in a safe environment facilitating trusted identities with maximum privacy. It integrates social networking persona with blockchain identities and national identity ecosystems such that the users controls access inside and outside the social networking environment to their personal information, communications, intellectual property and even their bank account and smart refrigerator. Identities, access rules and user authorization managed in the social networking environment of FreeTrust develop OpenID Connect identities trusted by the user and accepted first within trust communities with the potential to be accepted ultimately by global consensus. The distributed

social networking environment ensures privacy with end to end encryption providing a safe alternative to legacy systems like FaceBook and insecure email.

Economic model

FreeTrust aims to build a trust economy. Trust is not a medium of exchange. Earned trust cannot be spent. However credit may be issued based on trust. Payback for supporting FreeTrust is in fees associated with user activity. Fees are justified due to the value added to the network by the value of trustworthiness. Fees reward early investors and lead to sustainable enhancement, using fees to fund bounties offered by consensus of significant communities of users paid for over time by the fees they generate. Initial investments will claim a bounty as a portion of fees having diminishing returns after payback of value contributed. Given a constant level of network activity first payback of initial investment may be expected in say one month, paid again two months later, and again four months later, down to a unit of currency. Given exponential growth of the community the payback would be the same each month until the return per unit of activity falls below a unit of currency and payment stops. Fees also are applied to reward individuals having strong identity, presence, security and privacy trust factors since they enhance privacy. Fees also reward users for the use of their private information in proportion to the strength of the corroboration of their anonymous identity claims.

FreeTrust created it's own alternate currency, a privacy coin, privcoin. The currency will be convertible to any Dapp currency for the mashup of Dapp services employed by FreeTrust. It is designed to algorithmically maintain a trustworthy constant value such that it serves only as a medium of exchange and is not itself a commodity. Fees must be flexible so that they can cover the costs running the network as determined by the free market and pay for the rewards built into the system. The operational costs are expected to go down over time according to Moore's law. The network use of resources on the user's machine balances the cost of using the network such that only those using excess network resources will bear operational cost paying those who make resources available in excess of what they use.

The economics will include reward for strong corroborated trust factors of identity, presence, security and privacy since they add value to the network. The components of trust quantified by FreeTrust each will have exhaustive crowd sourced domain models for quantifying risk by maximum relative entropy (MrE) simultaneously applying Bayesian and maxent analysis to get a result, free of singularities, that is better than either method alone produces, using machine intelligence to quantify privacy trust risk factors from the trust perspective of the individual.

A small fee set by the owner of a personal information resourse in the form of a privacy coin is associated with granting permissions paid by the entity requesting the access permission to be granted inversely proportionally to their relative trust score and conditional on a user determined minimum. Fees associated with requesting a corroborated claim minus direct costs will be split among the owner and collaborators of the claim. Users forfeit fees and lose trust ranking if a

consensus is reached on a contradictory claim. In this manner value is added by correcting errors in identity information. Fees is split between the information resource owner and corroborators, bounty payments and the FreeTrust network to cover costs and provide the incentives for trustworthiness.

The economics will provide for subsidising basic access since participants add value to the network. The subsidy will be based on the strength of the trust factors obtained by the individual or other entity.. Subsidies cannot be accumulated but allow a limited daily credit balance to be allowed and forgiven. The more corroborated and longer lived identity factors they have, the stronger their authentication, the more secure their devices and networks are, and the better their privacy rating, the greater their daily subsidy. The daily distribution is intended to provide ubiquitous access to the network for identities while promoting a trustworthy cybersociety. Individuals will not have to pay to play.

The supply of FreeTrust currency in circulation is to be related to the value of the total trust earned by individuals in each of the trust components. It should roughly grow with the number of participants such that it maintains a constant trusted value.

In order that the currency maintain a constant value, the faucet, or rate of issuance will be throttled by market value relative to some fixed value such as the year 2000 dollar (Y2KUSD or 2KD) in order promote a non inflationary or deflationary value, if the value drops below the 2KD value the rate of distribution per identity would be increased, if the value go goes above a 2Kd the faucet is shut down as is necessary down to subsistence levels. These controls would be build into the system, algorithmically, without the possibility of human intervention in the spirit of Milton Friedman, JFK, Abe Lincoln, and Ben Franklin. Subsidies will be covered by the issuance of new currency or if necessary the distribution of fees to maintain a stable value of the currency.

This is an optimistic currency model that presumes an economy that grows at least in proportion to the population. It is betting that empowering individuals in the online world will enable them to create value. It suggests a consistency with Ben Franklin's notion that there should be just enough currency to meet the spending needs of the public and recognition that every strong identity in cyberspace brings real value to us all.

Architecture

FreeTrust is a distributed application implementing an interface to a mashup of APIs of existing open source distributed applications, installable by the user, which are already available to provide much of the required underlying functionality.

Synereo Dapp component

Synereo next generation distributed and decentralized open source Dapp system platform with peer to peer social networking provides extreme security and privacy by default in the user interface for managing authorization and trust relationships and provides intelligent user agent functionality of FreeTrust.

Identity Ecosystem Integration

Synereo puts security, identity, and privacy management directly under the purview of the user which will be integrated with User Managed Authorization (UMA, gluu, ForgeRock) in the national identity ecosystem and BitCoin style Blockchain identities employing transactions, smart contracts, distributed data layers, blockchains and federated consensus supported by other distributed applications such as eris, Stellar, Ethereum, Factom.

Social Contracts

Formal social contracts in Synereo, based on the pi-calculus, particularly those related to information disclosure, which are enforced within the social networking environment, will be exported to UMA rules and block-chain identities, using eirs/ethereum smart contracts and distributed data layer (e.g. synereo specialk, eris, factom) for immortalizing social and legal contract information. Eris “Legal Markdown” bridges machine contracts with human and legal contracts. Trust circles are built from the bottom up to organizations and connected top down from organization. Application to financial transactions will be demonstrated by integration of financial Dapps like Counterparty, Ripple and Stellar.

Personal Information Resources Services

User Agent

Collaboration Agents

Identifi Dapp component

Identifi is an open source Dapp which provides APIs for managing identities within Freetrust which will be gatewayed via SCIM and LDAP for integration with other FreeTrust componants and national identity ecosystems..

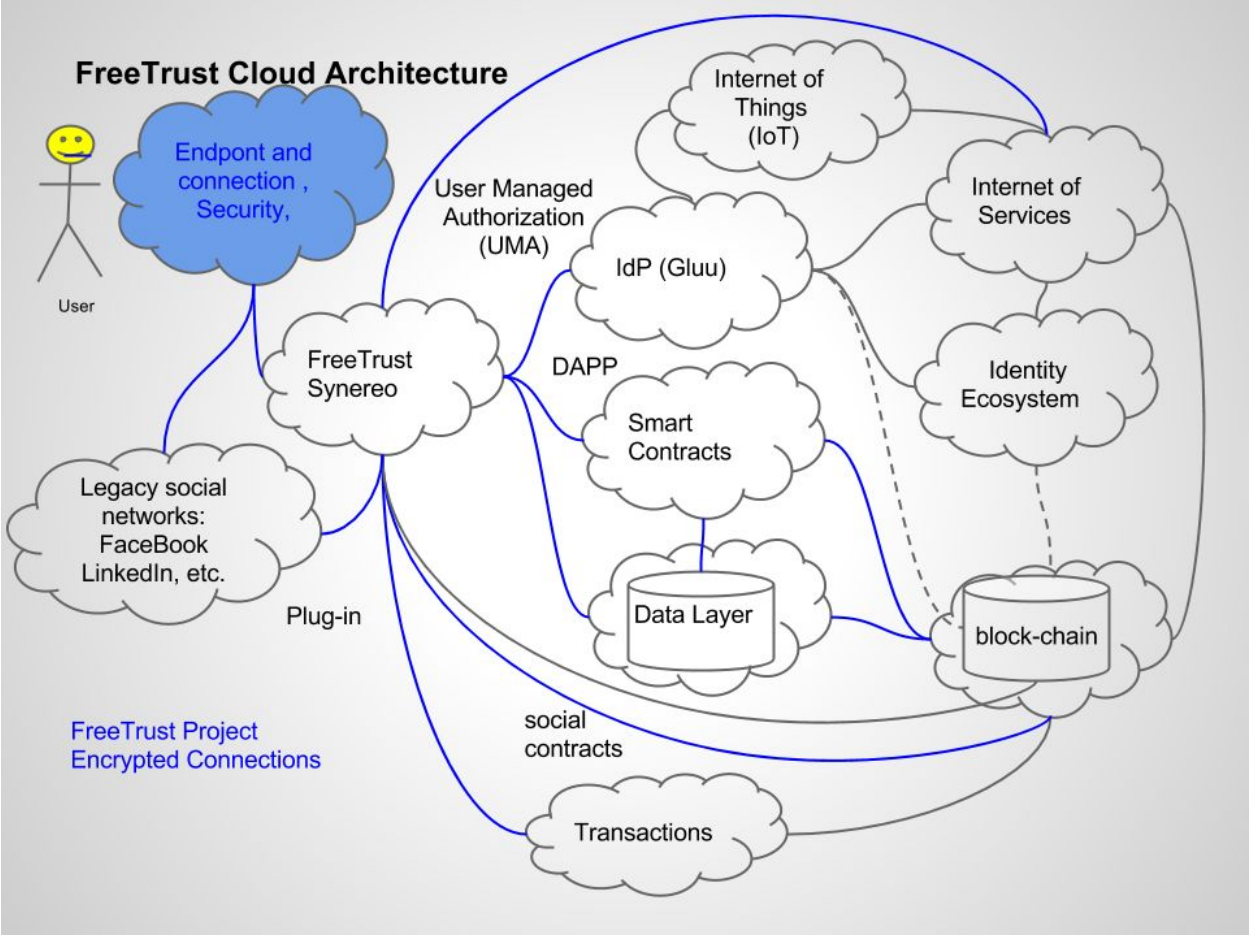
Each identity on the network may be its own PKI authority (CA, RA, and VA), having private “public” keys with exposure limited to trusted relations.

Eris Dapp component

Eris is open source software that allows anyone to build their own secure, low-cost, run-anywhere data infrastructure using blockchain and smart contract technology. It includes a fully-programmable, fully controllable, open-source blockchain database,smart contracts machine with a distributed application server that provides secure access to distributed applications with a simple API.

MrE Inference Engine

A maximum relative entropy (MrE) inference engine, prototyped by PSS under DARPA funding, will be employed to quantify risk in the trust of identity, presence, security and privacy according to user constraints to aid the user in making trustworthy privacy choices online and insure interactions have proven high trustworthiness. All possible vulnerabilities including the unexpected vulnerabilities are considered employing maximum entropy analysis user constraints and Bayesian experience Alternate inference engines, when they are available could be selected, as more trusted, by the user. The domain models for trust factor will be crowdsourced and inclusive with model selection by machine learning. Domain models will integrate related crowdsourced semantic web ontologies addressing the issues.



The system will be designed to evolve to interoperate with other Dapps and privacy enhancing mechanisms as they emerge. All system components delivered will be user installable allowing decentralization down to the individual, minimizing the target area to provide maximum security, ~~which may be replicated and protected by keys not stored locally and other privacy algorithms~~

Operational Pilots

ProvenSecure Solutions Inc. (PSSI)

PSSI will pilot FreeTrust internally and for customers of its planned ProvenId multi-modal claims-based authentication services. Utilizing advanced mathematical formulae based on Maximum Relative Entropy, MrE, we will implement a machine-learning system that fuses multiple authentication factors into a single ceremony, providing true Multifactor Authentication. We will also implement an Adaptive Risk Mitigation engine that can allow multiple sets of risk cards to calculate risk and multiple sets of threshold requirements for different stakeholders in the transactions, then merge the results into a highest common threshold.

Clarkson Pilot

Using a BIRTH CERTIFICATE voluntarily encrypted by/for the individual, the token then recorded to the blockchain with the individual's identity fused to it, is now available for verification that yes that is “the birth certificate token, and yes it has not been altered”. Various authentication factors can be associated with the token.

We already have the outline in place for an identity pilot with Clarkson University. This came out of the NSTIC proposal submitted with Ping360. This pilot would be different in that the document verification would use a “certified copy” of the birth certificate from the issuing authority verified together with the student in person by a notary or the University authority. Other authentication factors could be added at that time according to an accepted protocol meeting appropriate levels of assurance. A smart phone App could be developed for this purpose.

Clarkson University Pilot

Altrucoin

One domain that has gained traction in the crypto currency space is that of charities and “giving” models. The impact is extreme where the recipients of the giving have limited access to banking services, yet have access to cellular networks. Charities must be accountable to the donor, and the blockchain ledger provides an accurate record of the donation life cycle. ProvenSecure Solutions Inc. brings this model built on the FreeTrust platform as a pilot to emphasize the power of the trust networks in the Identity Ecosystem to address a multitude of real human problems in the real world. In addition, a revenue model ,which is essential to support the infrastructure, is also featured in this pilot.

WikiWorld

WikiWorld is a proposed FreeTrust pilot demonstrating the next generation internet where you are in control of your user interface, your personal information resources and are rewarded for your participation. Any groups sympathetic with the WikiWorld principles is welcome to participate with WikiWorld in the pilot.

WikiWorld aims to add value to FreeTrust with Dapp collaboration tools capitalizing on synereo social contracts and eris smart contracts for joint authoring (like fedwiki.org plus google docs), task management and group decision support.

links

http://www.coindesk.com/decentralised-apps-promise-new-way-business-online/
https://github.com/jkandah/Decentralized-Application-Business-Model/blob/master/README.md
https://github.com/DavidJohnstonCEO/DecentralizeDapplications/blob/master/README.md
http://www.wired.com/2015/04/stanford-prof-builds-algorithm-internet-money/
http://techcrunch.com/2015/01/18/after-the-social-web-here-comes-the-trust-web/
http://www.forbes.com/sites/ilyapozin/2015/04/10/meet-the-3-platforms-that-will-decentralize-the-web/
http://www.synereo.com/learn-more/
https://www.cs.umd.edu/~golbeck/pubs/Golbeck,%20Parsia,%20Hendler%20-%202003%20-%20Trust%20Networks%20on%20the%20Semantic%20Web.pdf
http://radar.oreilly.com/2015/01/the-3ps-of-the-blockchain-platforms-programs-and-protocols.html#
https://db.erisindustries.com/2015/04/28/smart-securitisation/
https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/
http://techcrunch.com/2015/04/03/be-your-own-bank/#.vm2vqb:3Dmo
http://en.wikipedia.org/wiki/Trust_metric
https://www.youtube.com/watch?t=53&v=hmfNfb_Rog4 Ian Grigg
https://blog.erisindustries.com/products/2014/12/27/step-by-step-eris/
http://www.statewatch.org/news/2008/mar/uk-nat-identity-crosby-report.pdf
http://www.wired.co.uk/magazine/archive/2015/06/features/bitcoin-reid-hoffman
http://jamieburke.co.uk/broken-trust-economy

Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age
by Winn Schwartau

Decentralised Apps Promise New Way of Doing Business Online
http://www.coindesk.com/decentralised-apps-promise-new-way-business-online/

Decentralized Application (Dapp) Business Model
https://github.com/jkandah/Decentralized-Application-Business-Model/blob/master/README.md

An Algorithm to Make Online Currency as Trustworthy as Cash
The General Theory of Decentralized Applications, Dapps
https://github.com/DavidJohnstonCEO/DecentralizedApplications/blob/master/README.md

After The Social Web, Here Comes The Trust Web
http://techcrunch.com/2015/01/18/after-the-social-web-here-comes-the-trust-web/

The 3 Platforms That Will Decentralize The Web
http://www.forbes.com/sites/ilyapozin/2015/04/10/meet-the-3-platforms-that-will-decentralize-the-web/

Synereo is designed as a framework for managing the economy of attention.
http://www.synereo.com/learn-more/

Trust Networks on the Semantic Web
https://www.cs.umd.edu/~golbeck/pubs/Golbeck,%20Parsia,%20Hendler%20-%202003%20-%20Trust%20Networks%20on%20the%20Semantic%20Web.pdf

The 3 Platforms That Will Decentralize The Web
http://radar.oreilly.com/2015/01/the-3ps-of-the-blockchain-platforms-programs-and-protocols.html#

DAOs, DACs, DAs and More: An Incomplete Terminology Guide

https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

Be Your Own Bank
http://techcrunch.com/2015/04/03/be-your-own-bank/#.kcfauq:vaFb

Trust metric
http://en.wikipedia.org/wiki/Trust_metric

CoinScrum and Proof of Work: Tools for the Future 2 - Ian Grigg - VIDEO
https://www.youtube.com/watch?t=53&v=hmfNfb_Rog4

From Blockchains to Eris: a step-by-step guide
https://blog.erisindustries.com/products/2014/12/27/step-by-step-eris/

The Broken Trust Economy
http://jamieburke.co.uk/broken-trust-economy

Reid Hoffman: Why the block chain matters
http://www.wired.co.uk/magazine/archive/2015/06/features/bitcoin-reid-hoffman

Challenges and opportunities in identity assurance
http://www.statewatch.org/news/2008/mar/uk-nat-identity-crosby-report.pdf

Your Next Passport Could Be On The Blockchain
http://techcrunch.com/2014/10/31/your-next-passport-could-be-on-the-blockchain/

Identifi

Abstract

Identifi [1] is a purely peer-to-peer identity & reputation database. The protocol is both security-by-design and privacy-by-design. All participants on the network have full control over any identity that they create. Each identity is a *First Class Person* [2] , which can be either a human or an entity (e.g., organization, corporation, country, computer, fridge, phone, drone, etc.). All identities can make claims about any other identity on the network. They also decide for themselves which other identities they want to communicate with.

The purpose of such a system is to create and organize reliable electronic trust networks, without the system deciding for any party which other parties are trustworthy or not. It is fully distributed both in its network topology and power mechanism. No sensitive information needs to be processed, nor sent, in order to reliably verify that the other party actually is whom they claim to be. This will help both humans and entities in weighing risks for themselves, before participating in any kind of interaction on a network.

[*Looking for people with a background in coding and academia to describe the data format, database design, network topology, etc., analyzed with practical results, of our proof-of-concept, here*]

Conclusion

We have proposed a system for electronic transactions that rely on trust. We started with the usual framework of trust made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent unreliable identities. To solve this, we proposed a peer-to-peer network using whitelisting to record a public history of claims that quickly become computationally impractical for an attacker to change if honest nodes control a majority of the network. The network is robust in its structured simplicity. Nodes work all at once with intelligent coordination. They need to be identified, since messages are routed to a particular place and don't need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the trust networks of trusted parties as proof of what happened while they were gone. They vote with subjective logic, expressing their acceptance of valid identities by working on extending them and rejecting irrelevant identities by refusing to communicate with them. Any needed rules and incentives can be enforced with this consensus mechanism.

Grigg's Ricardian Contracts

"*Describing digital value for payment systems is not a trivial task. Simplistic methods of using numbers or country codes to describe currencies, and ticker tape symbols to issue bonds, shares, and other financial instruments soon run into shortcomings in their ability to handle dynamic and divergent demands. The seemingly arbitrary variations in the meanings of different instruments are best captured as contracts between issuers and holders. Thus, the digital issuance of instruments can be viewed as the issuance of contracts.*

This paper proposes that the contract is the issue. A document form is described that encompasses the inherent contractual nature of the financial instrument yet copes with the requirements of being an integral part of a payment system.

(...)

Challenges for the Future

Layering. *Layering of contracts is an impending need. Many businesses can take a standard and defined set of terms and draw on them directly. Other contracts result from earlier contracts and need to reference them.*

XML. *Initial efforts suggested that XML would break the rule of one contract, but it seems that we will need something better than the archaic INI format. One recent proposal, the XML Voucher, stops short of presenting itself as a contract.*

Law of Contract. *The treatment of the Ricardian Contract as a contract may raise more legal questions than it answers. For example, is this form indeed a contract? How do distinct jurisdictions view the concept (common law, civil law, UCC, Koranic code)? Is this a negotiated or a form contract? When did the user accept the contract? How strong, or rebuttable, is the presumption that the user has the contract?*

Smart Contracts. *By unifying all information in a program-readable file, there is the enhanced potential of smart contracts. We have not gone further in this direction than methods to handle decimals. This is partly for lack of demand, and partly because it is not clear how a court would treat a computer program presented as a contract.*" [3]

Szabo's Smart Contracts

"*In this process of successive refinement we've gone from a crude security system to a reified contract:*

> *1.) A lock to selectively let in the owner and exclude third parties;*
> *2.) A back door to let in the creditor;*
> *3.a) Creditor back door switched on only upon nonpayment for a certain period of time; and*
> *3.b) The final electronic payment permanently switches off the back door.***"** [4]

Example of selling shares for BTC, by applying Identifi

Involved parties & identities

1. **Alice** (BTC holder);
2. **Bob** (shareholder);
3. **BTCshares.io** (platform on which they'll trade);
4. **PoormanStanley** (Alice's bank);
5. **DogmanSax** (Bob's bank);
6. **EchoTrail** (Blockchain analysis company).

Alice's identity exists of these identifiers:
Name = Alice (only 1 verification (by PoormanStanley), can be down-voted by 1M identities who are not trusted/verified by any party in this example, which are therefore irrelevant);
Country = US (also verified by PoormanStanley);
Bank = PoormanStanley (verified by PoormanStanley);
BTC address = 3BTCtradeAddress11 (verified by BTCshares.io via Alice's signature of 1/3 keys, and BTCshares.io also owns 1/3 keys);
Mobile = 555-ALICE (2 verifications (PoormanStanley and BTCshares.io)).

Bob's identity exists of the identifiers:
Name = Bob (only 1 verification (by DogmanSax));
Country = US (also verified by DogmanSax);
Bank = DogmanSax (verified by DogmanSax);
BTC address = 3BTCtradeAddress77 (verified by BTCshares.io via Bob's signature of 1/3 keys, and BTCshares.io also owns 1/3 keys);
Mobile = 555-BOB (2 verifications (DogmanSax and BTCshares.io)).

BTCshares.io's identity exists of the identifiers:
Name = BTCshares.io (3 verifications (Alice, Bob, and EchoTrail));
BTC address = 3BTCtradeAddress11 (2 verifications (Alice and BTCshares.io);
BTC address = 3BTCtradeAddress77 (2 verifications (Bob and BTCshares.io).

PoormanStanley's identity exists of the identifiers:
Name = PoormanStanley (2 verifications (Alice and BTCshares.io));
Business = Bank (2 verifications (Alice and BTCshares.io)).

DogmanSax identity exists of the identifiers:
Name = DogmanSax (2 verifications (Bob and BTCshares.io));
Business = Bank (2 verifications (Bob and BTCshares.io)).

EchoTrail's identity exists of the identifiers:
Name = Echotrail (1 verification (BTCshares.io));
Business = Blocktrailing (1 verification (BTCshares.io)).

Assumptions

For the sake of keeping the explanation of the concept as simple as possible, we'll assume that each party also runs a node (each node is a supernode and a key-server) themselves (no blockchain / sqlite3db == light-weight), and that Bob and Alice both use Firefox with an add-on that stores their privkey belonging to their identity (secure browser plug-ins are probably not the most secure implementation, so it's ment for the sake of keeping the example simple).

The “Selling shares for BTC” example

Alice surfs to BTCshares.io via her FF browser. She clicks on "login" to authenticate herself. She'll authenticate herself by signing a request to log on to the trading platform with her private key via the FF add-on, which will then be sent to BTCshares.io's Identifi node's API.

BTCshares.io verifies that Alice's identity meets the criteria (the pubkey has been verified by PoormanStanley), and can now make sure that it's her. They require a 2FA login, so BTCshares.io's node automatically sends a request to the node on her phone (to the public address of the node that's storing the identifier "555-ALICE" (each identifier also has its own public key)). Alice opens her Identifi app on her phone and taps the "Okay"-button, which is next to the request that she has received from BTCshares.io, just a moment ago. By tapping “Okay” on her phone, she verifies the login for a second time by returning the request, signed with the privkey on her mobile, to BTCshares.io. All demands from BTCshares.io for logging in have now been met. The session in Alice's FF now connects her to BTCshares.io’s trading platform.

Bob has logged in to BTCshares.io’s trading platform at some previous point in time, in the same manner as Alice did (the only difference here is that DogmanSax has verified Bob's identity), and he offered his shares for sale by signing his offer with 1/3 keys of the multi-sig address "3BTCtradeAddress77", which he co-owns with BTCshares.io. He also authenticated through 2FA via the Identifi node on his phone, when he put up the shares for sale. Bob has met all the criteria that have been put in place by BTCshares.io, in order for him to offer his shares to other users on the trading platform. This means that Alice will now be able to buy them.

Alice decides to buy Bob's shares, 10 of them at 1 BTC each. She enters the amount and clicks "Buy". She hereby sends a request to BTCshares.io to buy those stocks, and signs it with 1/3 privkeys of the multi-sig address "3BTCtradeAddress11" via her FF add-on. Once BTCshares.io has received her request, they now want to know if Alice has enough funds in her account, and if the funds on that public address are actually 'clean' coins. They check the co-owned multi-sig address and see that Alice has stored enough funds in there to make the purchase.

BTCshares.io now sends a request to EchoTrail, asking them if all the funds on "3BTCtradeAddress11" are 'clean'. EchoTrail takes their request, handles it, and returns the result to BTCshares.io. Their answer is "COINS_ARE_CLEAN", and thereby confirm that Alice's coins don't originate from any addresses labeled as 'suspicious' or above. BTCshares.io is paying EchoTrail for their services per API call.

The funds and shares are now both in place, the coins turn out to be clean, and Alice and Bob have agreed on the terms for selling the shares to Alice. BTCshares.io now takes the 1/3 multi-sig keys that belong to "3BTCtradeAddress11" to sign the request, thereby finalizing the payment to Bob. At the same time the 10 shares are being allocated to Alice's account on the trading platform.

/example

References

[1] M. Malmi, “Identifi”, https://github.com/identifi/identifi, 2013
[2] I. Grigg, “The Sum of All Chains - Let's Converge!”, http://financialcryptography.com/mt/archives/001556.html, 2015
[3] I. Grigg, “The Ricardian Contract”, http://iang.org/papers/ricardian_contract.html, ~1998ish(?)
[4] N. Szabo, “The Idea of Smart Contracts”, http://szabo.best.vwh.net/smart_contracts_idea.html, 1997