

How to be a person online : the RSA algorithm and Web of Trust

Presented by Robinson Dorion & Jacob Welsh

JWRD Computing – *Building Smart Tools for Smart People since 2016*

WoT: dorion, 54CCA1FC8C2E414C63BFB6CF0E48266E54D6B95A

WoT: jfw, 0CBC05941D03FD95C3A47654AE0DF306025594B3

Robinson's blog: <http://dorion-mode.com>

Jacob's blog: <http://jfxpt.com>

WWW: <http://jwrld.net>

Email: sales@jwrld.net

Slides : <http://dorion-mode.com/junto-how-to-be-a-person-online.pdf>

Wed, Jun 14, 2023

person (n.)

from Latin *persona* “human being, person, personage; a part in a drama, assumed character,” originally “a mask, a false face,” such as those of wood or clay, covering the whole head, worn by the actors in later Roman theater. OED offers the general 19c. explanation of *persona* as “related to” Latin *personare* “to sound through” (i.e. the mask as something spoken through and perhaps amplifying the voice).¹

¹https://www.etymonline.com/word/person#etymonline_v_12750

What is identity and how is it constructed ?

- Identity is the set of characteristics by which a person or thing is definitively recognizable or known.
- Identity is constructed, upon a fixed support, by others' view.

Fixed support example : your body


- Your family is the first to recognize you. They issue and attach a name to your body.
- They likely register you with the relevant governments in their environment.
- Government issues documents that acknowledge their recognition of you, e.g. birth certificate, passport, driver's license, etc.
- Lose one document, submit supporting documents and gov't issues you a new one, "password reset".
- Plus : hard to fake someone's body or face in person.
- Minus : Physical documents are "shared secrets". Once you share a copy your secret can be leaked and used in ways you don't intend to extract value from you/your identity.
- Minus : Issuing states can revoke your identity documents.

From Ludwig von Mises' Liberalism and Socialism, Ownership, annotated. on Trilema by Mircea Popescu

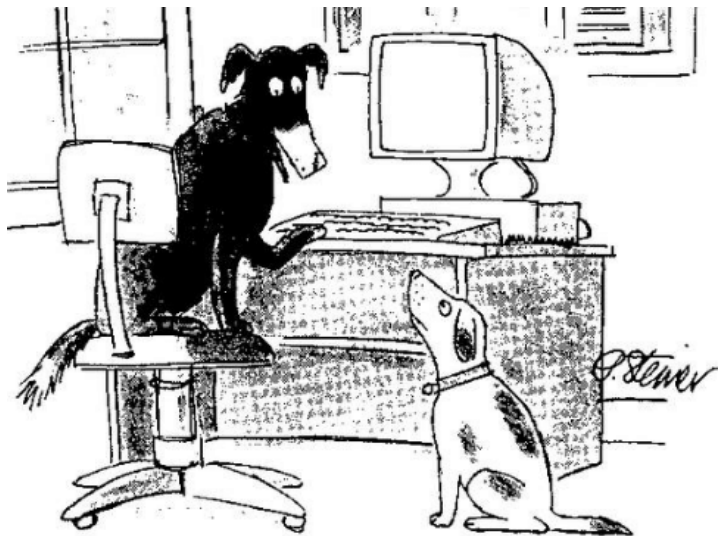
“An owner is correctly defined as he who may exclusively destroy an economic good... Once the owner is the only one able to destroy the good, his refrain from destruction then entitles him to demand the full price in exchange.”²

Do you own your passport or gov't ID certificates ?

Do you own your body ?

²<http://trilema.com/2013/lvm-lsa-i1ownership-1/> 

The challenge of identity on the Internet



"On the Internet, nobody knows you're a dog."

The challenge of identity on the Internet

- How do you know who you are talking to and signing contracts with on the other side of the wire ?
- How do you verify the sources of the software you are installing to manage your own data ?
- Have your friends and partners been hacked and impersonated by a bot ?
- As the bot army gets stronger, how will you know ?
- Are pictures of physical documents and hand written signatures a good fit for the Internet age ?
- Biometrics ?
- Computers are square key holes. They don't know who you are or what you mean, they just calculate.
- How can I enforce ownership over a given machine and its data ?
- How can I make sure a computer is *my* computer ?

The advantages of a strong digital identity.

- Write the strongest, hardest to forge signatures known to man.
 - Legal contracts are increasingly expensive to enforce and even moreso with the ultimate bearer asset : Bitcoin. “GPG contracts”³ and the WoT provide a structure for more economical contractual dealings.
- With one key, you get both signing and encrypting.
- If you can surmount the intellectual costs, owning your key is cheap.

Bottom line : What is owning your word worth to you ? What is privacy worth to you ?

³<http://trilema.com/gpg-contracts/>

The tools to build a strong, fixed, digital support.

- Entropy ;
- Strong Passwords ;
- Rivest, Shamir and Adelman (RSA) ;
- Web of Trust (WoT)

- Invented in 1977.
- Asymmetric/Public key cryptography.
- Leverages the computational intractability of factoring large numbers.
- Uses large prime numbers as the factors of the public key.
- What's big enough ? 2048 bit or 2^{2048}
- Example : which is harder, finding the prime factors of 13'843'867 or multiplying 2'029 and 6'823 ?

Bottom Line : Protect and safeguard a small amount of data as secret key material to enforce ownership of your identity.

How is ownership over the identity exercised and how is the WoT represented ?

- Exclusive control of a private key is one's sole claim to identity in the WoT world ;
- The WoT is represented as a graph, with nodes being the public keys of the participants, corresponding to private keys generated by the individuals themselves ;
- The edges of the graph represent the trust ratings between individuals, inbound and outbound, and consist of a sign (overall positive or negative trust), a number reflecting the rater's degree of certainty that the assessment will not change, and optional comment.

What happens if you lose your key ?

In the event that an actor loses his key, it's at the discretion of the other actors whether they want to verify a new identity for the purported person.

From the MPEX FAQ, #24 :

If either your account is very large and / or I know you I might try to verify you. Maybe. Don't count on it, but instead proceed with the clear state of mind that if you lose your keys you lose your assets. It's healthier.


from Trilema by Mircea Popescu

Trust isn't in the web or anywhere else but oneself.

The Web of Trust is merely the infrastructure upon which trust is built, by you, for your own use, within yourself.

The same objective set of relations can result in drastically different trust in the eyes of drastically different third parties.

The point of the WoT is not to make these judgements for you.⁴

⁴<http://trilema.com/2014/what-the-wot-is> 


The WoT works by reducing the unknowns problem.

from Trilema by Mircea Popescu

It allows the user - any user - to confidently identify the sources of information, both in the negative and in the positive.

That is to say, if sources of information exist, the user may by the WoT find them, and safely assume that should no sources of information be thus found, no sources of information in fact exist.

It further allows the user to judge the quality, reliability and precision of said sources, and this independent both of the direct source and of the counterparty he's examining.⁵

⁵<http://trilema.com/2014/what-the-wot-is> 

What are the origins of the concept ?

From 1992, the manual for *PGP version 2.0* by Phil Zimmerman

As time goes on, you will accumulate keys from other people that you may want to designate as trusted introducers.

Everyone else will each choose their own trusted introducers. And everyone will gradually accumulate and distribute with their key a collection of certifying signatures from other people, with the expectation that anyone receiving it will trust at least one or two of the signatures.

This will cause the emergence of a decentralized fault-tolerant web of confidence for all public keys.

- The three essential elements of an economy are : a **medium of exchange**, a **punishment gazette** and a **public forum**.
- The WoT serves as the punishment gazette as long as it can be inspected and not ever be modified.
- Business is built atop trust and credit and the WoT is a tool for conducting due diligence.
- Participants register identities and value is attached to the identities through interaction within the economy.
- Trust exists in the people rather than in the tools, but the tools provide the structure for making one's own judgments.


Personal responsibility and the Ponzi scam by Hannah Wiggins

Prosperity is in general the result of the working of free markets. The one caveat to this observation is that market participants have to be responsible. It doesn't matter so much if they are intelligent or not, it doesn't really matter if they're good christians or devout muslims or anything else, but they do have to be responsible.

When some people behave irresponsibly the result is that they lose their money, which flows, albeit indirectly and circumvolutedly but nevertheless unerringly, to more responsible participants.

When a small majority* of participants behave irresponsibly however the net result is not just pain to their own fortunes, but pain spread across the board. All of a sudden you have to be very intelligent, and very experienced, and very well informed to manage to keep your money safe, and often enough even that's not going to suffice.⁶

Bottom Line : An effectual punishment gazette incentivizes people to act with greater responsibility.

⁶<https://bitcointalk.org/index.php?topic=106391.0;all> 

How do the ratings work ?

- Ratings range as integers from -10 to 10 and include an optional comment.
- Ratings are not school marks or facebook likes or amazon stars, they are statistical dampeners.
- The only thing someone's score tells you is how likely it is for you to have someone who knows him in your network.
- How well am I acquainted with this guy ?
- How valuable might my input be to a third party asking for references ?
- The thinking capacity of the users makes it valuable.

How do the relevant actors communicate ?

In the forum, which for the biggest chunk of Bitcoin's history meant IRC and the "libraries" aka blogs of the participants.

The forum and its implementation on Trilema by Mircea Popescu

The public forum does not serve the function of "allowing communication", just like that, indistinctly.

The participants are sharply divided between the relevant and the irrelevant, whether they know this or not, and whether they'd be inclined to accept it or not.

Communication, which is to say bidirectional information flows, happens between the former. Towards the latter information flows unidirectionally : they have nothing to say. Whether they know this or not.⁷

⁷<http://trilema.com/2014/the-forum-and-its-implementation/>

- PGP by Phil Zimmermann
 - Came from a context where away from keyboard, in person relations carried more meaning.
 - Allows users to vouch for “validity” and “trust” of a key owner.
 - Validity signifies that the name in the key’s metadata matches the owner’s legal name, e.g. verified by checking documentation.
 - Trust signifies whether the signer trusts the owner to do a good job of verifying the identities of other people before signing their keys.
 - Signatures are issued upon the ratings given.
- Bitcoin OTC by nanotube
 - Owner : nanotube
 - Ratings : a scale ranging from -10 to 10 with an optional comment, verified by the issuer with a valid response to an encrypted challenge.
 - IRC channel : #bitcoin-otc and #bitcoin-assets on Freenode
 - Bot interface : gribble
 - WoT viewer : <https://bitcoin-otc.com/trust.php>
 - Website : <https://bitcoin-otc.com>
 - Cause of Fork : the service went offline and nanotube went unresponsive, more details here : <https://archive.is/4FuFv>

Bitcoin-Assets implemented by Matic “kakobrekla” Kocevar

- Ratings : a scale ranging from -10 to 10 with an optional comment, verified by the issuer with a valid response to an encrypted challenge.
- IRC channel : #bitcoin-assets on Freenode
- Bot interface : assbot
- WoT viewer : <http://www.btcalpha.com/wot> by mike_c⁸.
- Website : <http://bitcoin-assets.com>
- Origins :
<http://trilema.com/how-bitcoin-assets-was-born/>
- Cause of Fork : In the wake of a controversial transaction related to BitBet (MPEX : S.BBET) an irreconcilable rift between Mircea Popescu and kakobrekla was uncovered.

⁸Archived : <https://archive.is/QIDkE>

#trilema

- Ratings : a scale ranging from -10 to 10 with an optional comment, verified by the issuer with a valid response to an encrypted challenge.
- IRC channel : #trilema on Freenode
- Bot interface : deedbot by Michael “trinque” Trinque
- WoT viewer : <http://wot.deedbot.org/> by trinque.
- Website : <http://trilema.com/2019/introducing-the-logs/>
- Cause of Dissolution : Mircea Popescu closed⁹ the TMSR project, essentially because not enough of the soi-disant Lords stepped up to put skin in the game and not enough new blood could be found to replace them. (Technically, this manifested as ongoing infrastructure maintenance problems much like before.)

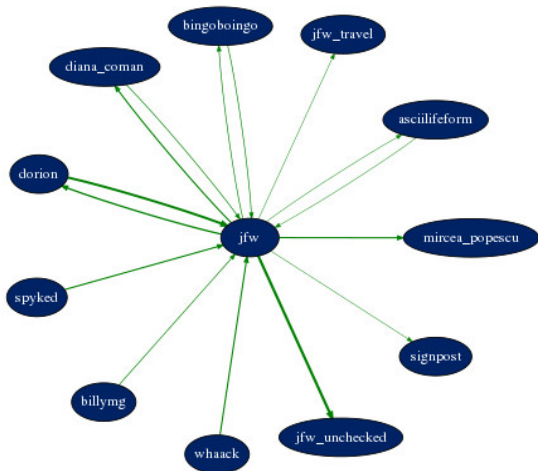
⁹<http://trilema.com/2020/closure/>

JFW's Trilema WoT graph

jfw

Fingerprint

[0CBC05941D03FD95C3A47654AE0DF306025594B3 \(quality\)](#)



JFW's received ratings in the Trilema WoT

Ratings Received			
Rating	From	Timestamp	Note
9	dorion	2020-03-01 12:03:33	my best good friend and business partner for many years. Writes at fixpoint.welshcomputing.com . Gales Linux, Gales Scheme, Gales Bitcoin Wallet, etc.
5	spyked	2020-05-26 02:05:08	jwrdr; huge pile of tech work: gales linux, scheme, gbw etc.
5	whaack	2020-03-31 12:03:29	Met in the flesh, writes at fixpoint.welshcomputing.com , has a wealth of knowledge about computers, bitcoin, and the like. Made a linux distro and wallet tool.
3	BingoBoingo	2019-12-07 05:12:09	Met in person. We rolled servers on the rambla.
3	billymg	2020-04-26 10:04:10	smart CS guy, currently digging into TRB, in addition to working on his own wallet and OS. provides valuable code reviews. working with dorion to educate otherwise smart/wealthy individuals on how to properly use computers. writes at fixpoint.welshcomputing.com
3	diana_coman	2020-03-30 04:03:03	YH member, JWRD consulting; sysadmin; Gales; writes at fixpoint.welshcomputing.com
2	ascilifeform	2019-12-11 04:12:43	maths fella, industrial FG user.

What did the WoT enable for Bitcoiners ?

- Effective collaboration.
- Thriving commerce and investment.
- Governance of Bitcoin itself.
 - The “blocksize debate” was resolved swiftly and intelligently in the forum of adults using the WoT.
 - In the various reddits filled with n00bs, the echoed bleating of a “debate” carried on for years which resulted in numerous forks which all predictably failed.

- Eulora2
 - Eulora2 is a masterclass masquerading as a video game, players will likely trade and develop commercial relations.
 - Identity : following the S.MG communication protocol, Eulora2 uses RSA identities.
 - Ratings : scale from -10 to 10, with a comment field.
- JWRD-WoT
 - The implementation details are yet to be determined, but we will encourage the use of RSA keys secured via Airgapping.
 - Code authors and signers who want to contribute to our projects will be required to register a key with us as a minimum for consideration.
 - We are participating in Eulora and using that WoT. However, being a client-server video game, the Eulora2 identity must be on a machine that's connected to the Internet.
 - Will start via IRC and likely migrate to Eulora2 in the future.
 - Ratings : scale from -10 to 10, with a comment field.

- As the bankrupt fiat legal and monetary system continue to devolve, what can one do ? What can one control ?
- You can control the tools you pick out of the options available.
- You can control the people you build relationships with.
- As the bot army and zombie horde strengthens online, what are the most effective ways to leverage the Internet ?
- Will you develop yourself to become the owner of your voice and word online ?
- Will you build your defenses to ensure it really is your friends and partners on the other side of the wire ?
- If you don't own your name, your word, what do you have, in the end ?
- Call to action : register you GPG key in the JWRD WoT and join the forum on IRC, read more here :
<http://jfxpt.com/grand-reopening-of-jwr-d-the-irc-channel/>
- JWRD provides hardware, software and training to save clients time and money in establishing themselves, read more at <http://jwr-d.net>

Bottom Line : if you're a person, prove it.

Thank you for your time and attention !
Questions and comments are welcome.