



Neue Geschäftsmodelle mit Blockchain

Prof. Alfred Taudes

Dr. Christian Baumann

KMU DIGITAL

WKO
WIRTSCHAFTSKAMMERN ÖSTERREICHS

bmwfw
Bundesministerium für
Wissenschaft, Forschung und Wirtschaft

Abgrenzung Bitcoin / Blockchain

- „Satoshi Nakamoto“: Whitepaper 2008
 - „Eine elektronische Währung, die auf einem kryptografischen Beweis beruht und kein Vertrauen in Mittelsmänner benötigt ... damit ist Geld sicher und kann mühelos transferiert werden.“
 - Kernthemen
 - Peer-To-Peer (P2P) Netzwerk
 - Verteilte Datenbank
 - Konsens ohne Vertrauen
 - Start Bitcoin Blockchain: Jänner 2009
- Bitcoin = Erste Anwendung einer Blockchain
- Blockchain-Technologie für andere Anwendungen verwendbar

Blockchains - Hauptmerkmale

- Dezentral („Peer To Peer“)
 - Blockchain auf alle Teilnehmer verteilt
 - => Alle gleichberechtigt, keine „Zentrale“
 - Datenbank, Netzwerk sehr robust (Ausfallssicherheit)
 - => nicht (bzw. sehr schwer) zerstörbar
- Transparent
 - Konsistente Sicht auf alle Daten
 - „Eine Wahrheit“
 - Vertrauen durch Kryptografie („Digitaler Fingerabdruck“)
- Unveränderbar
 - Neue Daten nur hinzufügen
 - Bestehende Daten unveränderbar/unlöschar
 - Vertrauen durch Kryptografie („Digitale Signatur“)

Kryptografie

■ Kryptografie 1 - Digitaler Fingerabdruck

- Hashfunktion, Blöcke, Blockchain - Live-Demo (*)
- <https://blockchains.web-lab.at/bc-demos/blockchain/hash.html>

■ Kryptografie 2 - Digitale Signatur

- Schlüssel, Digitale Signatur, Einsatz in der Blockchain - Live-Demo (*)
- <https://blockchains.web-lab.at/bc-demos/public-private-keys/keys.html>

(*) Original: Anders Brownworth - <https://github.com/anders94> - Anpassungen/Erweiterungen: C. Baumann

Kryptografie - weitere Anwendungen

- Keypairs & Hashverfahren
- Blockchain intern
 - Signieren von Transaktionen
 - Hashwerte der Blöcke => Verkettung
- Zusammenhang mit Daten/Dokumenten
 - Daten
 - verschlüsselt in der Chain speichern
 - nur ausgewählte Empfänger können entschlüsseln/lesen
 - Dokumente
 - „offchain“ transportieren/verspeichern
 - Hashwert als Bestätigung in Blockchain
 - (Speicherplatz, Datenschutz ...)

Ausprägungen von Blockchains

Je nach Einsatzzweck, 2 Dimensionen

- Zugriff („Wer darf lesen?“)
 - Public: Jeder Client darf (komplette Blockchain) lesen
 - Private: nur bekannte (geprüfte, authentifizierte) Teilnehmer
- Validierung („Wer darf schreiben?“)
 - (Transaktionen verarbeiten, Blöcke bilden und hinzufügen)
 - Permissionless: Jeder Teilnehmer
 - Permissioned: beschränkte Liste („Konsortium-Chain“)

Dimensionsmatrix

		Validierung (schreiben)	
		<i>Permissionless</i>	<i>Permissioned</i>
Zugriff (lesen)	<i>Public</i>	Bitcoin, Ethereum ... PoE (öffentlich)	Register, Zertifikate ... (veröffentlichen)
	<i>Private</i>	(n/a)	Banken, Versicherungen „Konsortium“ (intern)

Smart Contracts - „Verträge in der Blockchain“

- Programmcode, der vereinbarte Regeln abarbeitet
 - In der Blockchain gespeichert, läuft auf den Nodes
 - transparent, unveränderbar ...
- Eigenschaften
 - „selbst ausführbar“ - „wenn - dann“ - automatisch
 - „selbst durchsetzbar“ - „unstoppable“
- Interaktion mit
 - Blockchain: Werte empfangen/sendern, auf Ereignisse reagieren
 - Außenwelt: Sensoren, Aktoren über Schnittstellen („Oracle“)

Blockchains - Stärken & Schwächen

■ Dezentral

- Keine Zentrale („Mittelsmann“) nötig
- Nicht zensierbar
- Kein eindeutiger Systembetreiber / Kein Systemverantwortlicher

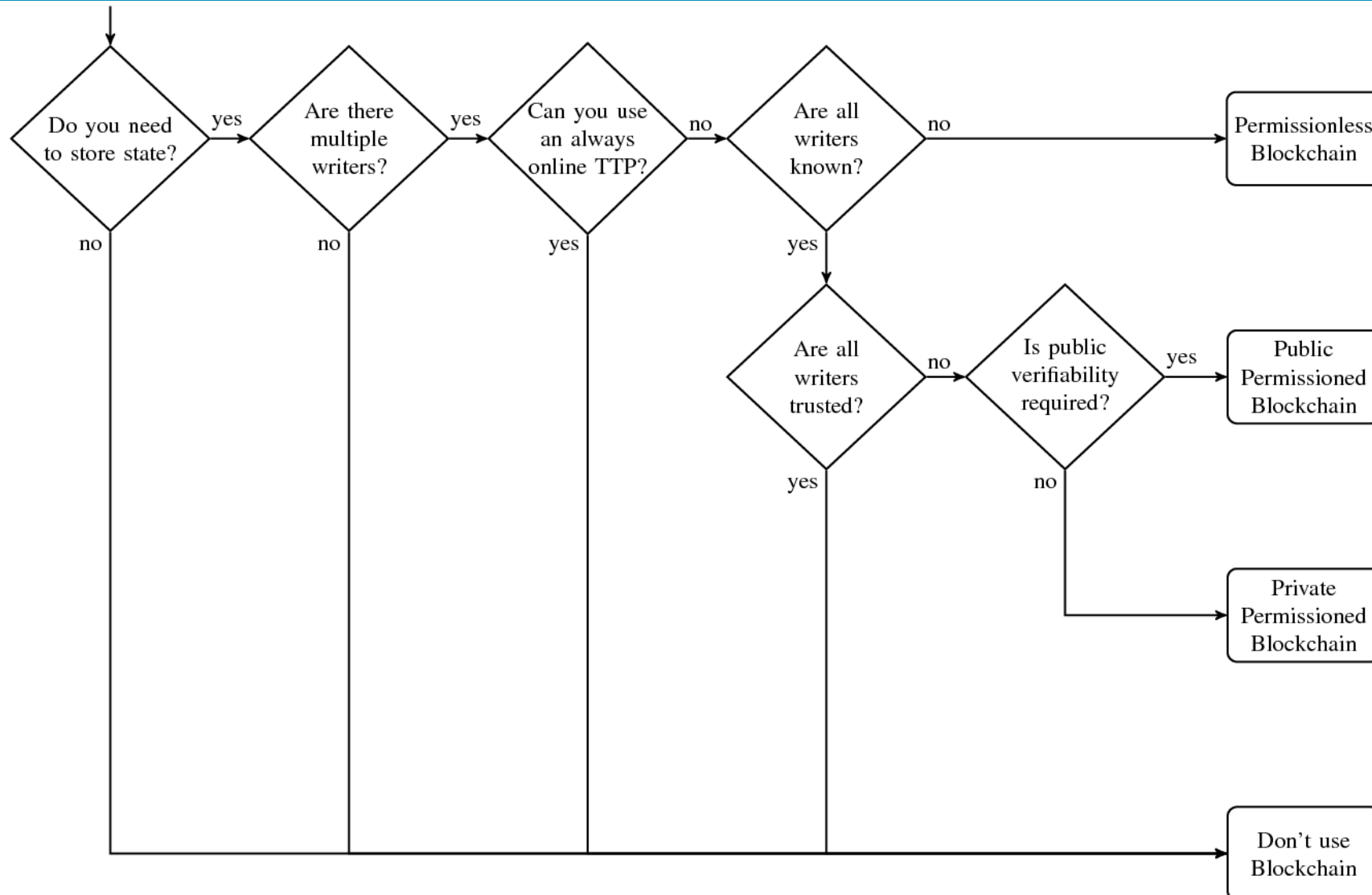
■ Transparent

- Konsistente Sicht auf alle Daten, „Eine Wahrheit“
- End-To-End Verschlüsselung zwischen Teilnehmern möglich
- Transparenz nicht immer erwünscht

■ Unveränderbar

- Unlösbarkeit => Datenschutz? (DSGVO)

Do You Need a Blockchain?

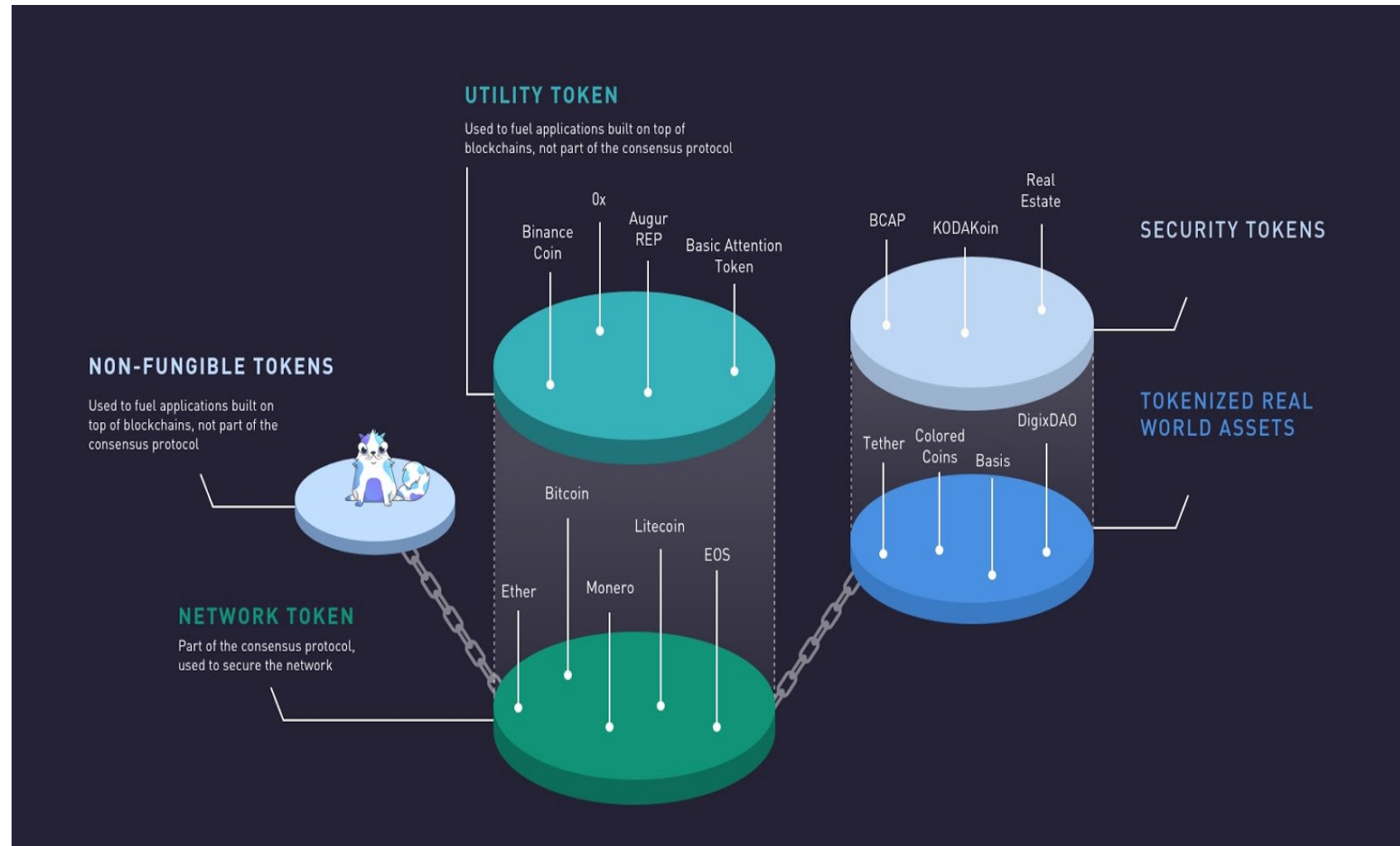


Wüst, Karl, and Arthur Gervais. "Do you need a Blockchain?." 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE, 2018.

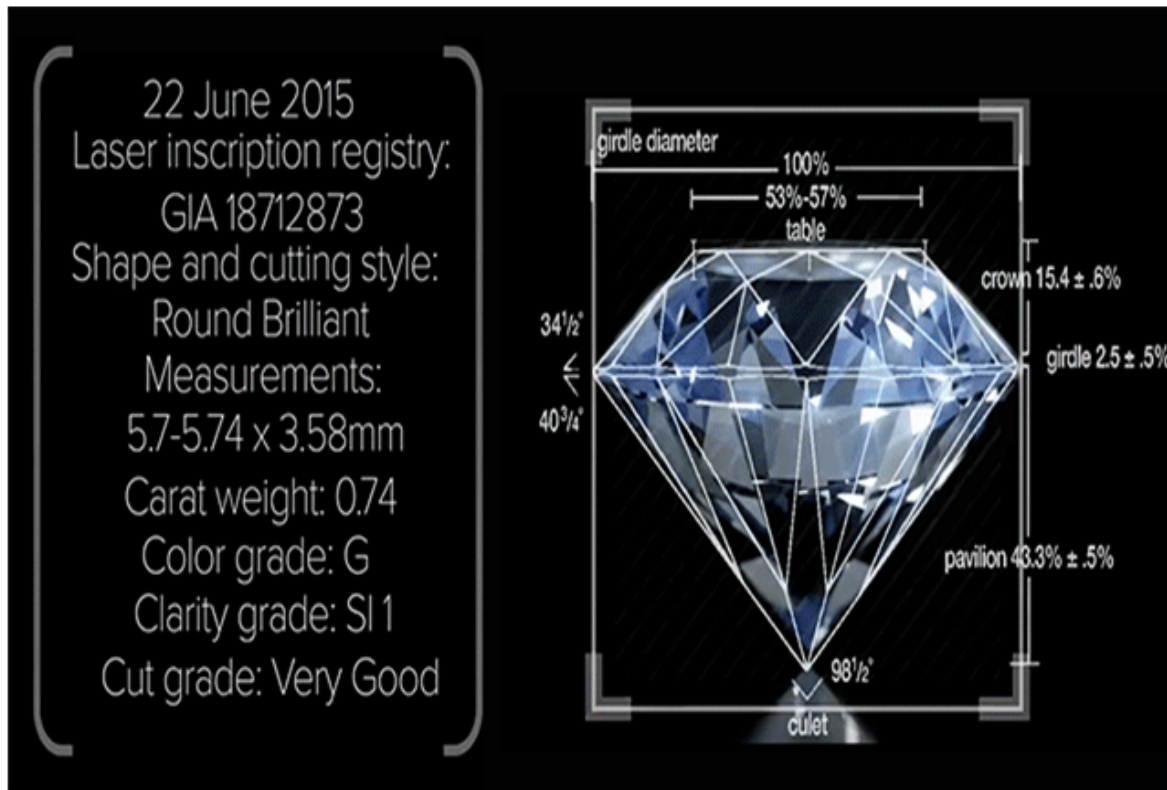
Kerneigenschaften in a Nutshell

- Notarfunktion
 - Supply Chain: Echtheit, Verfolgbarkeit, Effizienz
 - Qualitätssicherung
 - Identität, Datenschutz und KYC
- Smart Contracts
 - Finanzdienstleistungen
 - Gaming
- Token
 - Social Media
- Handel
 - Wertpapiere
 - Energie

Token Types und Internet 3.0

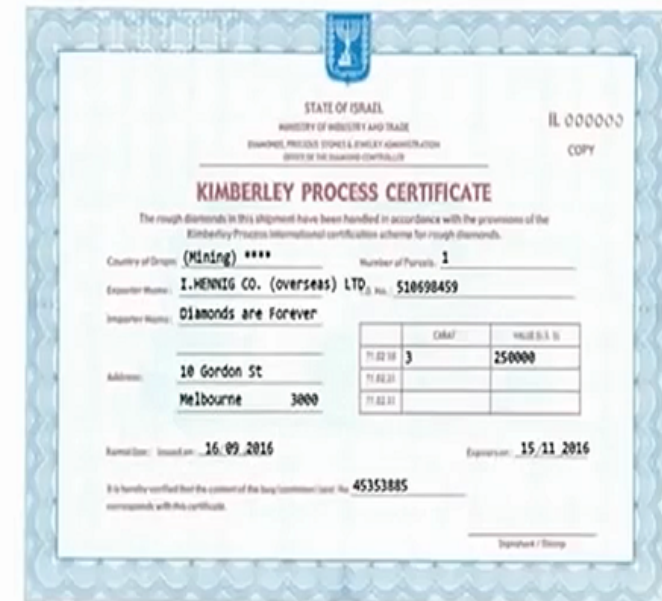


Everledger



Andrei Croitor (andrei@croitor.co.uk)

Please verify you have received the following shipment:



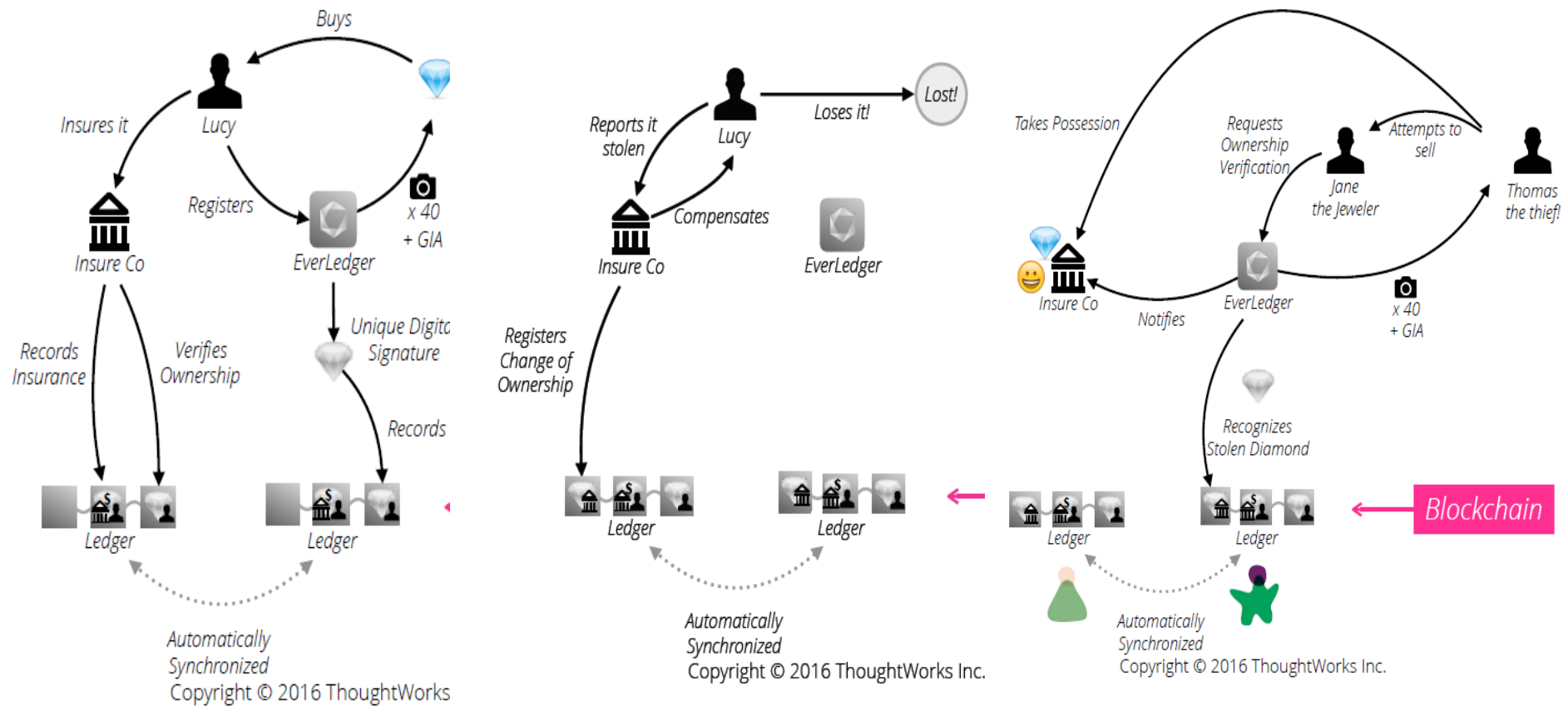
IL Nr
Invoice Date KX123444234

Bag / Parcel #
Invoice Number 45353885

Reject

Verify

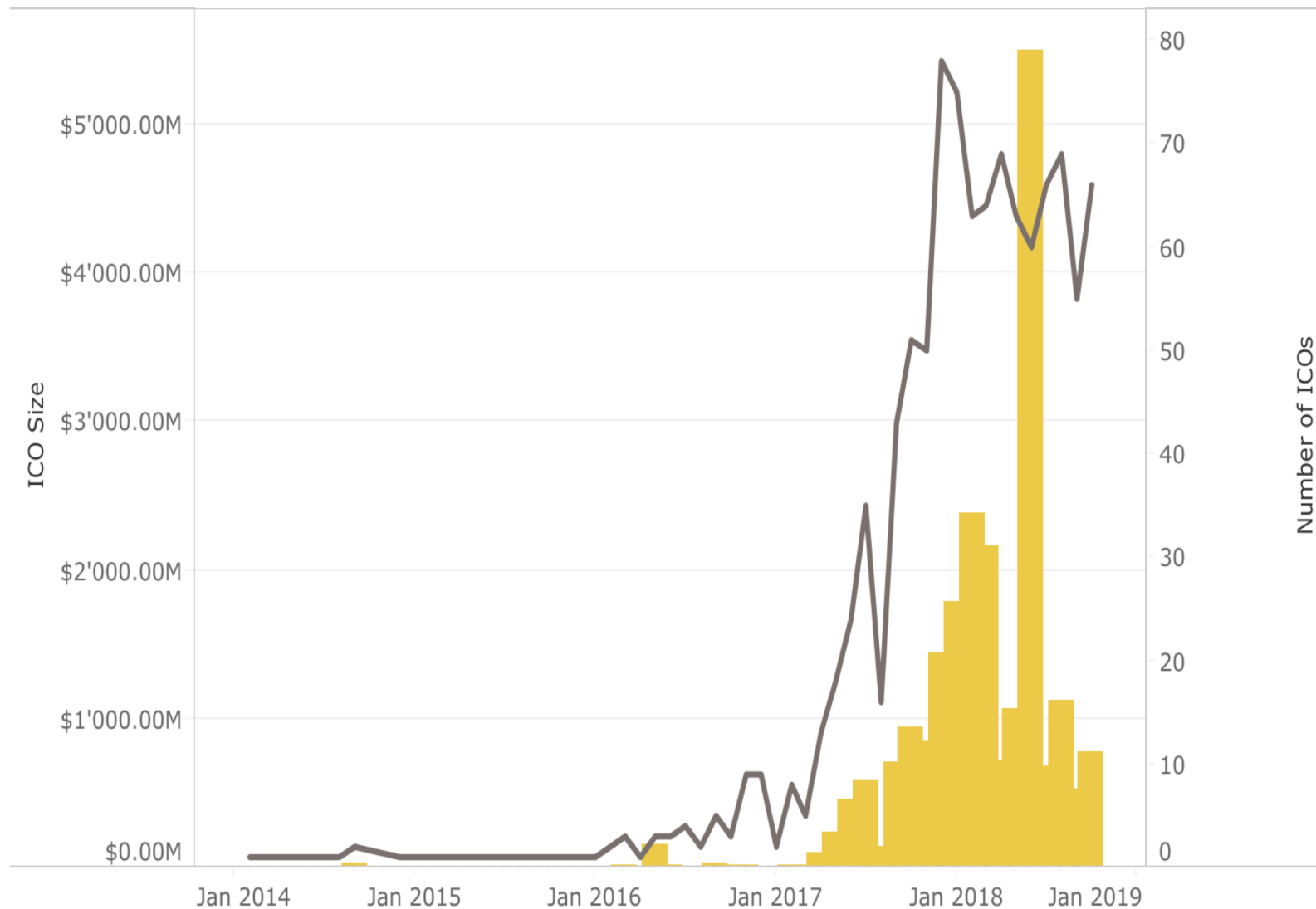
Everledger



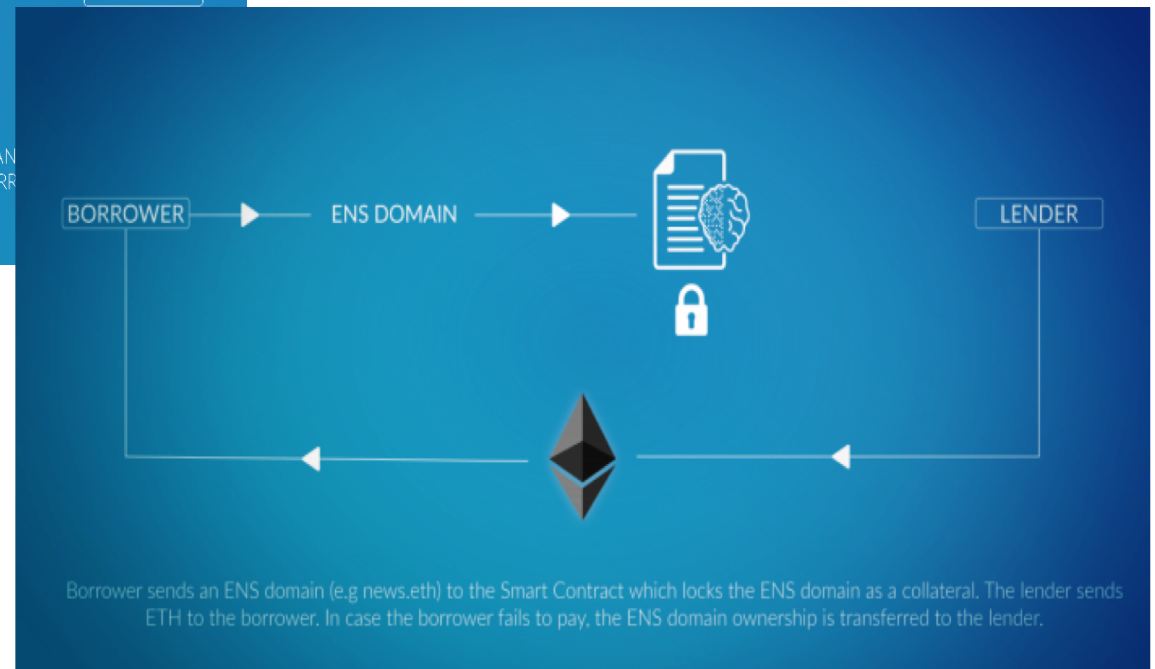
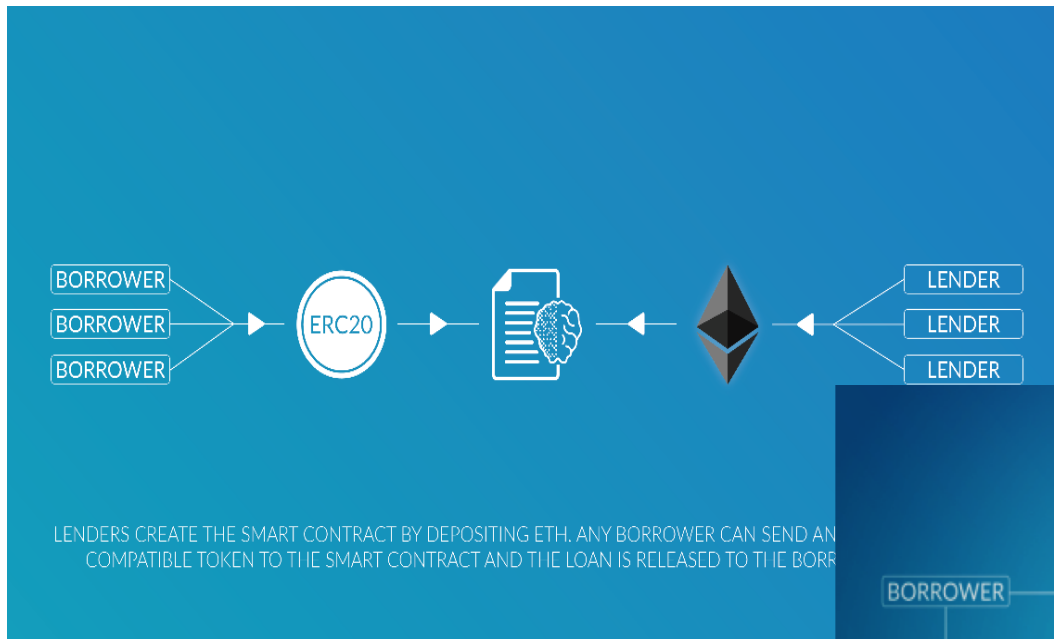
ICO Volume (16 in Österreich)



Monthly New ICO Funding



EthLend



Flugverspätungsversicherung

Apply for Policy

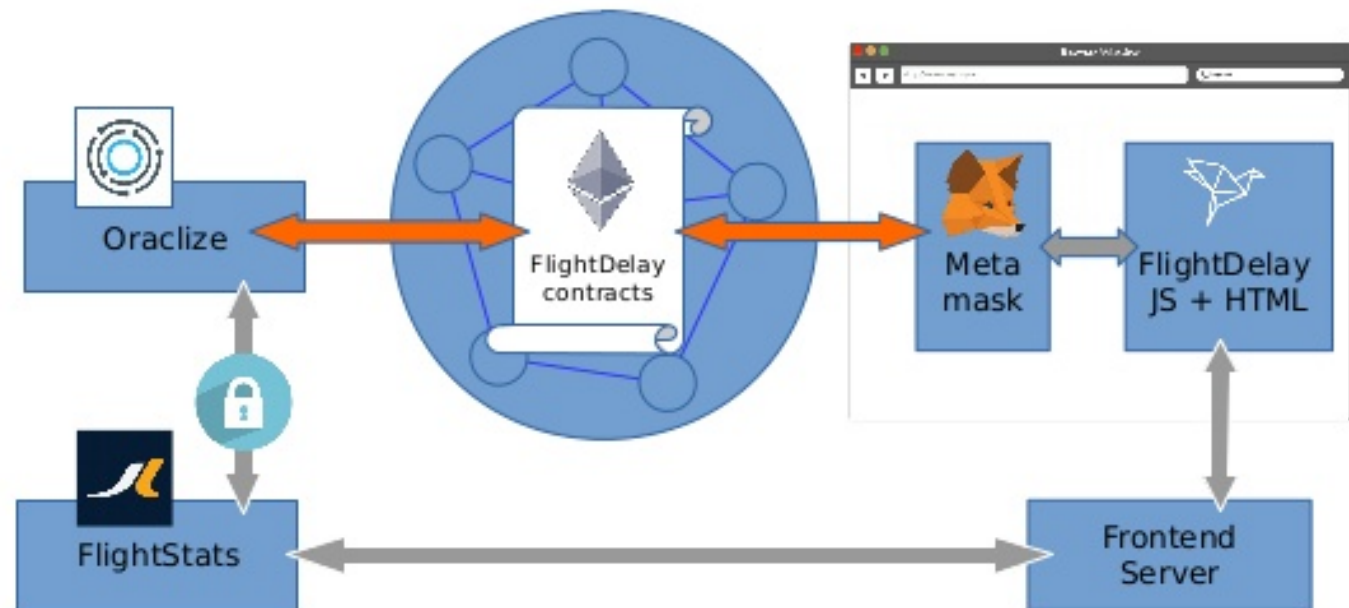
First name Last name

E-mail Date of birth

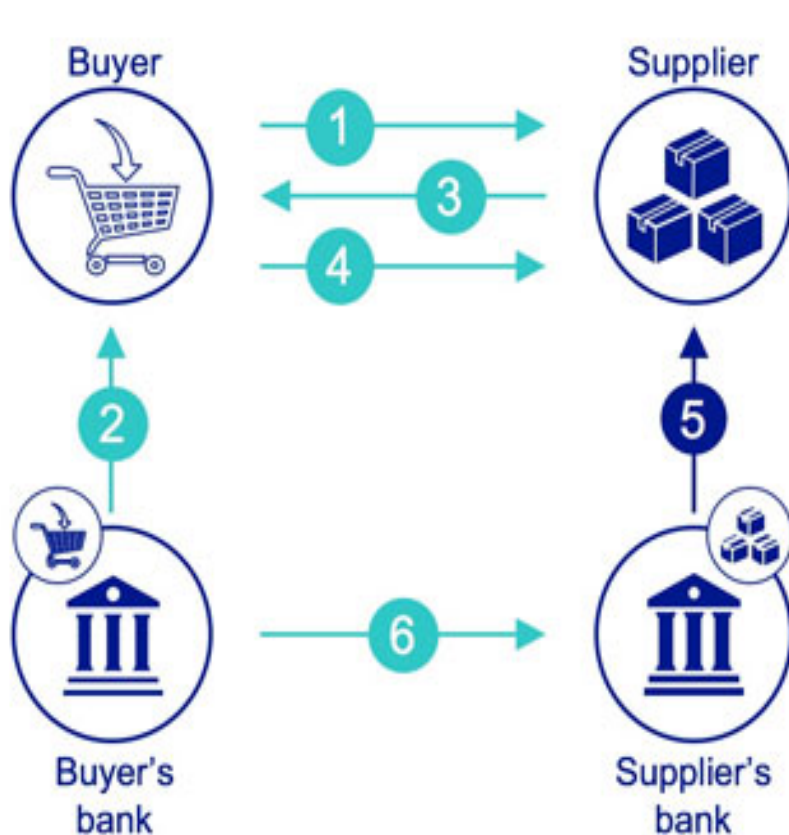
From To

Content in this frame is delivered by Atlas Insurance PCC Ltd, a company licensed to transact general insurance business in Malta. Authority. In respect of any contract concluded via this site, you are dealing directly with Atlas in Malta and consequently the risks covered are those of Atlas in Malta.

General architecture

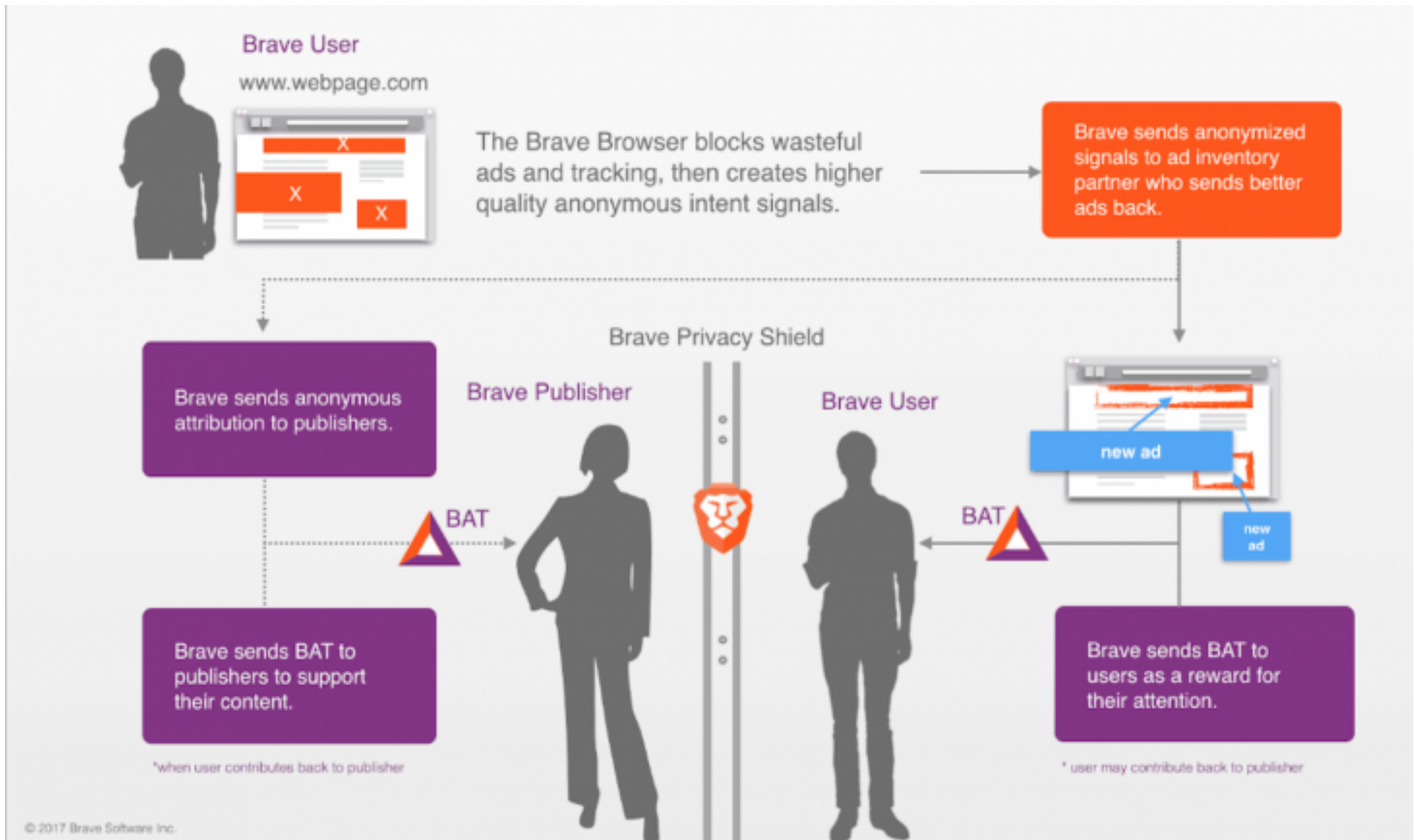


We.trade



- 1 Buyer initiates purchase order with 60 days payment terms
- 2 Buyer requests bank to provide Bank Payment Undertaking (BPU)
- 3 Supplier ships order and sends invoice through the platform
- 4 Buyer confirms the receipt of goods
- 5 Supplier asks his bank to provide invoice financing arrangement for next 60 days (optional)
- 6 Buyer's bank debits buyer account and initiates payment of invoice on due date, either...
 - to supplier's bank, if invoice has been financed **or**
 - to supplier's account

Werbenetzwerk



Social Media



Trending New Hot Promoted

Login

Sign up



All tags

life
photography
kr
steemit
art
bitcoin
introduceyourself
spanish
travel
cryptocurrency
food
steem
busy
blog
funny
news

Trending: All Tags



dahaz159 (68) in ezira • 13 hours ago



Ezira Hangout #19 | Ezira: State of the Network | 2018-8-12 | 1PM UTC

Ezira combines blockchain social media, with a decentralized ex...

⬆️ \$784.02 ⬆️ ⬆️ 709 ⬆️ 51 ⬆️



badkarma619 (59) in dtube • 11 hours ago



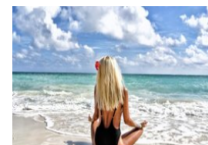
Bad Karma feat Nipsey Hussle - Colour Blind prod by Sandy 3ps

Shout out @Sixoneninetime, @Heaterville, @Smartmediagroup ...

⬆️ \$669.39 ⬆️ ⬆️ 335 ⬆️ 14 ⬆️



kevinwong (75) in witness-category • yesterday



Running for Witness: Embracing the Crypto Life™

Dear Steem community, Recently over coffee, a friend asked me...

⬆️ \$839.06 ⬆️ ⬆️ 812 ⬆️ 167 ⬆️

New to Steemit?

Quick start guide
The blockchain
FAQs
Sign up

CryptoKitties



CryptoKitties ● Network Good

Catalogue

Search

FAQs

More

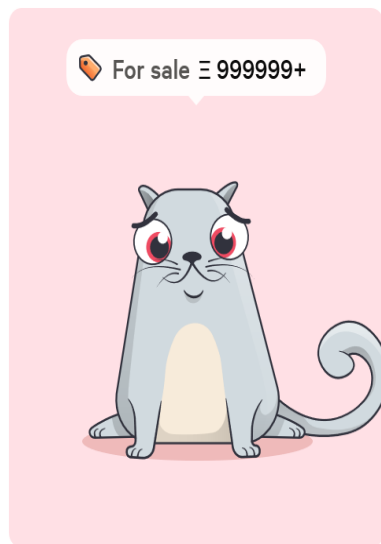
Start

Search

filters

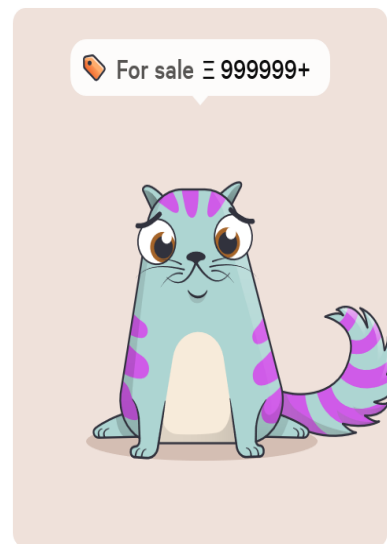
☒ for sale ☐ siring ☐ other

sort by price high to low



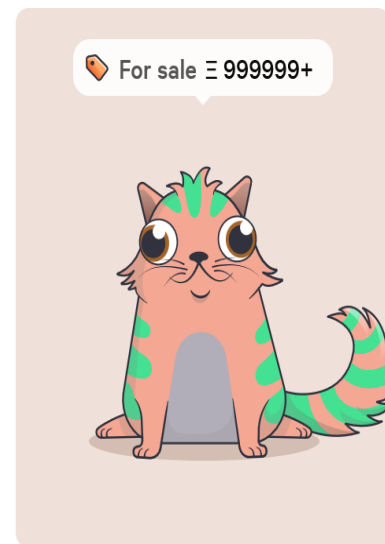
193760

♡ 40



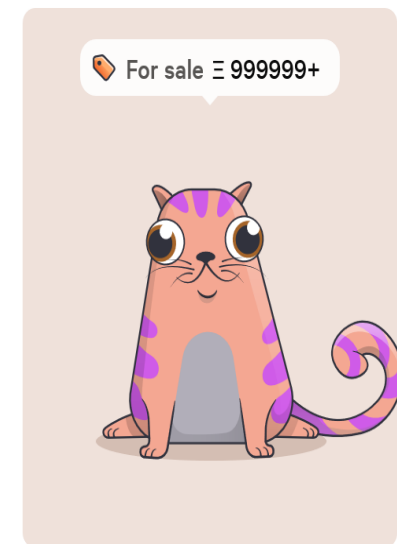
58177

♡ 28



151911

♡ 22



193659

♡ 31



Risiken

- Unreife Technologie
- Durchsatz / Responsezeit
- Hohe/unsichere Transaktionskosten
- Viele Alternativen
- Know How
- Rechtliches Umfeld
- Netzwerkeffekte und Lock-in

Vorgangsweise

- Technologie verstehen
- Suche nach geeigneten Einsatzfeldern
- Prototyp und POC
- Öffentliche Testnet / Cloudinstanzen
- Start Small
 - Periodisches Notarifizieren traditioneller Datenbestände
 - Transaktionsabwicklung
- Integration mit Frontend, traditionellen Datenbanken, Sensoren