



# Smart Contracts

## The Future Of Dispute Resolution?

Professor Michael Mainelli  
Chairman, Z/Yen Group  
17 March 2022



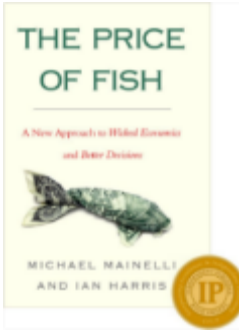
@mrmainelli

[michael\\_mainelli@zyen.com](mailto:michael_mainelli@zyen.com)

[www.zyen.com](http://www.zyen.com)

# City Of London's Leading Commercial Think-Tank

- ◆ Services – projects, strategy, expertise on demand, coaching, research, analytics, modern systems
- ◆ Sectors – technology, finance, voluntary, professional services, outsourcing
  - *Sunday Times* Book of the Week, **Clean Business Cuisine**
  - Independent Publisher Book Awards Finance, Investment & Economics Gold Prize for **The Price of Fish**
  - British Computer Society **IT Director of the Year 2004** for PropheZy and VizZy
  - DTI **Smart Award 2003** for PropheZy
  - £1.9M **Foresight Challenge Award** for Financial Laboratory visualising financial risk 1997
- ◆ Innovation – policy performance bonds, prediction markets, medical imaging, support vector machines, low-loss electric cables, risk visualisation, smart ledgers, etc.



# Agenda

A prophetic meeting at my offices in 2016...

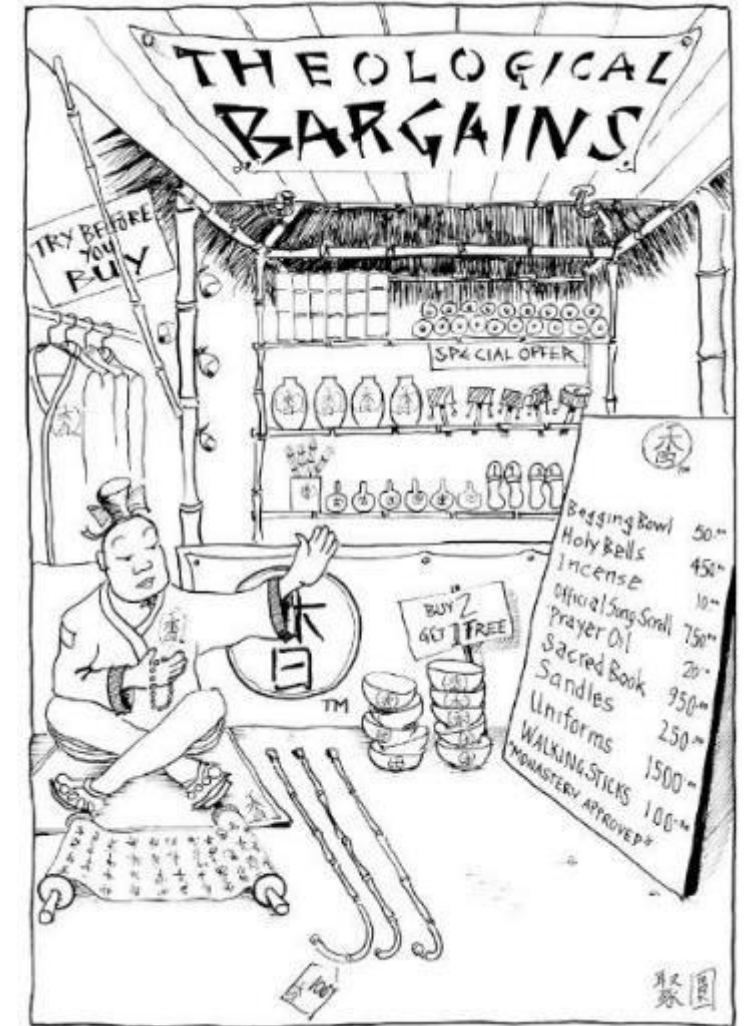
- Beyond The Blockchain Bandwagon
- Overview of Distributed Ledger Technology (DLT)
- Overview of Smart Contracts and thus Smart Ledgers
- Some prejudices
- Smart Ledgers – What's a poor arbitrator to do?
- Q&A



**"Get a detailed grip on the big picture."  
Chao Kli Ning**

# Why 'Smart' Ledgers?

- ◆ Smart ledgers (aka blockchains, distributed ledgers, mutual distributed ledgers) are:  
“multi-organisational data structures with a superb audit trail and some embedded code”
- ◆ Smart Ledgers are touted as a technology for fair play in a globalised world - numerous project announcements (and marketing hype) from governments, financial firms, shipping firms, large IT firms, and the like



**"Get a detailed grip on the big picture."  
Chao Kli Ning**

# The Old Old New New Thing...



[www.dilbert.com, Friday, 17 November 1995]

[Internet (1976 for me), databases (Oracle, Ingres, DBII, relational/hierarchical/distributed), web (SGML, Gopher), 'Internal Internets' (i.e. intranets), social media (SixDegrees)...]

# Buzz or Hype? The New New Thing

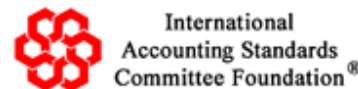


[Ken Tindell mashup - 14 May 2015 <https://twitter.com/kentindell/status/598865133247569920>]

# What Is A Central Third Party?



**Validates – entries**  
**Safeguards – transactions**  
**Preserves – historic record**



# Why Do Central Third Parties Exist?

*Financial services are based on 'mistrust', leverage, and pooling*

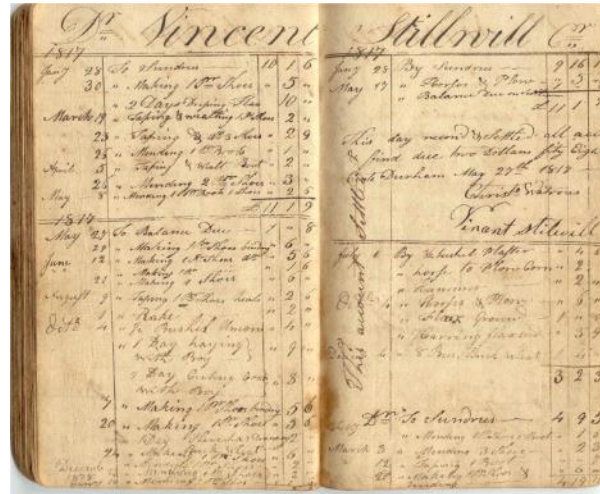
- ? Validate - Sin of Commission – forgery of new member or asset
- ✓ Safeguard - Sin of Deletion – reversal of a transaction
- ✓ Preserve - Sin of Omission – censorship of a transaction





# What Is A Ledger?

“A ledger is a book, file, or other record of financial transactions.”



Christopher Watrous Ledger Book, Durham, 1817 (Vedder Library)

Accounts for Demo  
CASH ACCOUNT From 01/03/2003 to 29/03/2004

Date	Payee	Reference	Category	Actual (gross) Amount	Recon Balance (gross)	Admin. fund split OST net	Non OST	Sink. fund split OST net	Non OST	Balance (net)
25 MAY 04	Mr J Citizen	Lot 1 levy pa	Deposit	500.00	500.00	0.00	500.00	0.00	0.00	500.00
26 MAY 04	Local Insurance	Insurance	Ar Insurance Bu	-269.00	231.00	0.00	-269.00	0.00	0.00	231.00
31 MAY 04	Netbank	Govt Debit Tr	Govt Debit Tr	-2.52	228.48	0.00	-2.52	0.00	0.00	228.48
31 MAY 04	Netbank	Account Ser	Account Ser	-5.00	223.48	0.00	-5.00	0.00	0.00	223.48
31 MAY 04	Netbank	Interest	Bank Interest	0.52	224.00	0.00	0.52	0.00	0.00	224.00
3 JUN 03	Clarks Grounds	Grounds Mai	Grounds Mai	-30.00	194.00	0.00	-30.00	0.00	0.00	194.00
10 JUN 03	Electrical Engine	Replace light	Building Maint	-22.60	171.40	0.00	-22.60	0.00	0.00	171.40
11 JUL 03	Levy credit trans	Lot 1 credit	Levy credit tr	0.00	171.40	0.00	-250.00	0.00	250.00	171.40
10 OCT 04	Leahy	Terror Payou	Bank Transf	1000.00	1171.40	909.09	0.00	0.00	0.00	1080.49
10 OCT 04	Fencers Upstand	Broken Pain	Fencing	-120.00	1051.40	0.00	0.00	0.00	-120.00	960.49
16 OCT 04	Mr P D Jakeson	Lot 1 levy pa	Deposit	400.00	1451.40	0.00	0.00	363.64	0.00	1324.13
6 NOV 04	Mr P D Jakeson	Lot 1 levy pa	Deposit	25.00	1476.40	0.00	0.00	22.73	0.00	1346.86
11 NOV 04	Mr P D Jakeson	Lot 1 levy pa	Deposit	5.00	1481.40	0.00	0.00	4.55	0.00	1351.41

[SOURCE: [https://en.wikipedia.org/wiki/Tally\\_stick](https://en.wikipedia.org/wiki/Tally_stick)]

[SOURCE: <http://www.rootsweb.ancestry.com/~nygreen2/wpeF7.jpg>]

[SOURCE: <https://en.wikipedia.org/wiki/Ledger>]

# Modern Ledgers aka Databases

- **1960s:** IBM Develop Hierarchical Databases to store information, taking advantage of new storage capacity, e.g., SABRE, IMS Network Model also developed, but fails to become widely accepted.
- **1970s:** Codd's Relational Databases proposed, allowing search by content and more flexible relationships, e.g., INGRES, System R.
- **1980s:** Increased computing power allows Relational Databases to become dominant, e.g., DB2, PARADOX, RBASE 5000.
- **1990s:** Object Oriented Databases followed by Internet Database Connectors allow different types of data to be stored and queried, e.g., Oracle, Access, ODBC.
- **2000s:** NoSQL – high performance, highly scalable, denormalized data takes advantage of distributed storage and fast connections, e.g., Cassandra, HBase, Neo4j.
- **2009 - present:** Bitcoin, cryptocurrencies, DLT, MDL, etc.

“Smart Ledger Patents & Prior Smarts”, Michael Mainelli and Henry Price, Digital Bytes, TeamBlockchain (27 May 2020), pages 8-11 - <https://www.longfinance.net/news/pamphleteers/smart-ledger-patents-prior-smarts/>




# What's One Look Like?

## Metrognomo Live Ledger

UUID	MetroTime	RowHash	TableHash	Tag
d426bb4c3dbd4ea6a44ae5ef56a2e40a	2022-03-17 17:48:44.068580	3a6170ffd15edd01f7ea93f37a73ec1d4fa4f5460c417991bbd84f7bbd9104f1	6894c436aaea9a2f02f9bf92630c3958e6aa02527852fe851934b45e94ab5c9d	hJzB_H83hWGQgTaVw-T91cxE-B2DLUj8Ow6R0XNdin6h6wflTE_Liw===:lBaHaF-MVABxRPiXKrP_sXz6qELjr-CDW9ZDKeGq348=
e38b37864d444e5fa90303fa96cd6781	2022-03-17 17:49:13.379387	46be9d3a3ff63363193d352b3a0b9714718e21cc24f15f919b5e35c22453b4aa	7462c291d5d67c8078749689d0975544efa50bbc5b51ae36f43419de15294109	Jw2xr8_3kr3sYBpn8GIFTTsxESaL4v_xTM3qxEG3bGHY8m2Q797TGOs0=:0CYWb7WV6yq52a36nSs1vvWTI3PJ3bUIr7vmX70bf4=
a7a751b1d43f494bbc3250b5b7f23c12	2022-03-17 17:49:16.060953	d9243432faaf85c1012c16e36b82e5730e133efe1d27fb59e51ccebcb5dd7ad92	2d1e974a1aa5a83b75ef91f95d8a4cfe0c9ce13823edff6f85ede1d71336c6	YGSeCwNGf8aFa8QsEX1x8n7sVDhQSYz2XVX9rQSjv:LNsdVtdBMkCE=:U17YWhmpkUKoeb78bDCCZqsV7DbmZ9jgARfeuiNb78I=
39cc69a988824f1b8800824bcf118034	2022-03-17 17:49:26.397200	51075cbf493f5f928c62561376b43c27880ff89acbedd88872656d972e12e	2ebd72bde0ed1db93822afe697dfe8c4e72c663de70ea2304098ad88326c9e76	KqITQaplhp7vgTrpglpPkP_V84IbC3M3FQOipfoBoOcYGYXf4C_Q==:OSprky-7nuQW5iNTQhQ8j32FdAYRbHlvi6b4on2lec=
d5769846aabf4d75a14c925db7bd028f	2022-03-17 17:49:35.359256	9f1de13d0f6dac6f7789736da354335845596dff097691433b589c6e3d3e4c4	55b55f02e27a8935a25c67c468bc1578c095d005aaab12104ca2123a109e850b	2fSLS2OQfvrUL69KCIr_Pk0SwGVxSE0-dEiHFRxuyNZIGSTHoIepM5L:OokjrSzWg3LUMeMSJDYv8BFopstCjwj91YBk6h1B48s=
7331a2b5e25f4e62afc0b315fe22d9e5	2022-03-17 17:49:37.866173	ccbe39dcaea1b1e4508eacbd7a502031165eb38952774e630692fa1d347b9734	052e54b2c16632d5ced76a309ad1c3ea4808a2632ef2f3fdb0db2dfa13a13b93	-QeF35B4pzq9ufRQOwocXFD3BSwG-6vppRro4QrhcMbPyOB:rk8sGqdJXUaFTUGJI3NZdSDTjzozYkr:8GMvEDpZXXvw=
f2f13660592d42af8deeb41be53b9c8c	2022-03-17 17:49:41.045495	9bbd0de38b111295a1676f9360dd1dc92538eea3a635af5172a2a0a1cd26828	9f00797059cefbb24ef14b5ca6e73850abb957655f7ebe997ede486a5b7d74f1	gdze_vb4gtUX8O6M9_rcVOrle18QWVY3E4OQdRGobZz-ChMg3e1T1ZU45yc=:wElipyYur-PLC5o2IXfhd_a2dKMDWNZAsO-G_QmrWh0=
a20c7e5f547f43d3bb35547625b3a94f	2022-03-17 17:49:44.276882	6d0e99eaa5e9ba9e056b8089262aea0982091a135bdcaed56c4165b9f5b349d	8eba8e977760c4587275c50a42d8f4fea60d130c127859f68d47ae90b04f92ec	HbPhJ7D5HwQ6GSmBtdgVY7pF7y0ZNYsusut2Vp6y9Is3nNn5UT2nb0u7OFME=:AUHuZIG_br31cY2g3RtgMla9TiA1EoQkeKznLv_OjRc=
7648c058ae2e4dbab5d0955dab82fb04	2022-03-17 17:49:53.065952	17b9a89c1528ce20c9af1fda6d2946e0286f2875db5586699e730ca23b2267	6d645e564347b2387ec68b48a53f8cbe28e838d3ba83293b72bd000490beebc	MLxI3FuJ6Kj6Yx-1Hd21GiovtSbXsE1_o1-cDauwaoPLRWzbqSo=:Idjtm9dtnFuevU_105qTJdqOTeUuo_nY61W30_IRMU=
90cebfdccb404970b1d4627b38f17979	2022-03-17 17:50:00.010410	068734609b05473f5d1495b101d50a40f6124d4519eaf7fa0265fe7690876ad	cdeaf8018549ac973f6c5c418b23e6a53071a162a0a63e601a5e05f405c79348	HrTKMOex517t1Ww:2CW5cSxRqZZaE3D1j7lQfIc2ia_oBI3HWpASvCbWg4hUBA==:8VYcX_Zwqos1Oltg5arOAJ2vMTCgk-ihP1W017_Ouis=
451996c0f47f416ca49b1808424db80f	2022-03-17 17:50:25.130966	1dfc385319d6886c81c83f3eb0a06e6e87841df36713cd594ce8f676afb497a	295e1dc211c130a1d862c1f1d8c5d121e5168f6424fb5b098f49f02d8077093c	KSXypRknPQXUJH_utWmPdSPbCmH9A2vOFU2HRvrPgVq4xg==:_Gfl3zsbcrR_kCXOp06WVOP5jsliRgS2pOM1HGtm8w=
eca6f9f451f1436cae1ca225707076f0	2022-03-17 17:50:38.143528	4bd7408aa8ca9ac80a5506f90543bd7312bf9b5f15893b761ecc48e3333d83ac	55800f63171a202126b2897becf98b5082e7659e65c279d2aafe45fcef3c2a	vIZB8rQpNbfFGi2oIpuyy4nAqKECEG5T4R:A9DsSxrNe2e-DHCG6lkqz4g==:cwdottjaYjB9pJWV_qo1WHf6o6Zf9Ev3ArmBpXsNRjs=
b1ae5788f896437ab5fa5bb006e5f215	2022-03-17 17:50:40.849293	3d913afd83132aa4b146e4b1230a73803b810daacb127fe5d3dba194a6de1a5a	8a521a15b04509baef7c1b72715d159ca445ca86a02114a76593ba668ebf3a19	zkUHggIqGVN6gCaWkFdhonHofobuJOIneK21WEBjMYdWqXavefYJow==:h4Xv:FmVny6JbfpnsB5sfO_RzK3mFW0dQ3pXo51SaWVtk=
186d1cec689a4a5b872482115edb45a3	2022-03-17 17:51:33.491596	b0b1e75d9561342eafd258db64696ca7a587b1d46ac818839a43ffaf0bda737	944828a5d32027eb521c3e86bf9107ad35b68f2a7c4fea0e4ac07b50ab6ac7a	k0tks2GWcInL10eWRAQ1kjKov5WwtjgJcf_5Sh67TQDKNspMaI=:SgkB23M317bVz0c-EIvzXn136BQAcT8bHC7FyW9InQ=
b2fe9f673e4a4964ae66b17fc09adba	2022-03-17 17:52:56.234145	ac0e3d55006143b13f51a3e713fa4f9b00c575442b780804ad9020294a1c9924a	4941dfed5a1815b7345af8c3ef025ebb0a97cd8feb3b73ef51062b53338f0c06	PsGR6RuSCE_ppVrgwJEH6mOyJGHjOxo2bmj98pbowheVbMfwB6WNk=:e2KIH_m1njfIdfA1imiYhtTQz-OcLs56qLU32jyC2_4=
bba1c6ab4b0445ceb1c53a0e13eff3c	2022-03-17 17:52:59.506768	7f8074844f04cb608dc38d59ca4b3c766aa9ea662d076259d2292fd3d00f0f	232cb0e6ab7c76de30719400a4f269023b0add8d83f825c4c8f6f13b39fcf268	1YhXwZnu4S6tqRBvIw_4ZSeqN1yi7MFwr0TPCEWLIWHZ8ffg8-3HIOf1:-1q4cRA2w5B8cnUHGm7oqKA9JOkv_X_6_9nXvu9H98K0=
c19fd62c67a422e88cf4fb6276eff3f	2022-03-17 17:53:05.168564	0574e724d09fae1b0b582fc101941c5f5e1b1d4fda2bbd1238db7f5e12ef280	6aac9e9e5e51d12cb9425b151467e504eed9b13c3121dfc3f41eeaa0c289745	LwJy3ubEdYgxfXz2An2S3RmrSJrcMHP9iJLuALSE9XLbyL:IKmR8ayTrzkLLZegRZcmigbp8afipzayYt1HkftgEgI=
76c77cd7271342f4b41944bda548fe3e	2022-03-17 17:53:29.290047	b6322dbf2aeaddb955824ef07ca4782802c7c77d4555b31a5206ea5b90925b5bb	6f22f5ff9864abff56e3df2085742a057542beaa4452466ce1db25e0b87cd834	Zs9sgAjhnrVuCSHzHMqSSs8e9ibPcfQ_fDSiGMxGNXkI7A1xwY2f7lYhYg==:z8aiAbP33LT9znwZ68icCcCpJ4JbTP7iULzHqOelv0=
6ad8d5e1a2dc486d8470811f7301f88c	2022-03-17 17:53:31.517190	b8586e478a9b0d7ebb4c7e6e33c4f35a61882883439ee225aa2e65d4fd28d701	fedd767c85e7ec7a081cb38b83df83716e8d2b577fb458f678a1d76119d7fd89	MRr46-VYBIPgQWVpH0B6C1a61-b2_vZXOKc6EI_SnlXxNgQPqt0CG8VVnOk=:0LYBa8xKL_JOymcMACvS9zBMZi-9Q3e4pIYVONPqopg=
1dfef5a192cd4abaa235d8bd1a898050	2022-03-17 17:53:33.853071	95b0564d9f03a7f719f561b9a3d0864049ec61e99a4f78543b45dc23631f24f	c42681837296ac293b27a6aa7155247cd31414a3b39783167c4336d9ce32ac8b	HLDSdgjEi1GUuW5Wwug8mY7EgfCqiVduH74Qj8fj68FqTmqj11Od4=:Kwc5JE2kTXG6o56T1SubBf8NWKJONHBUfy0aRecKCU=

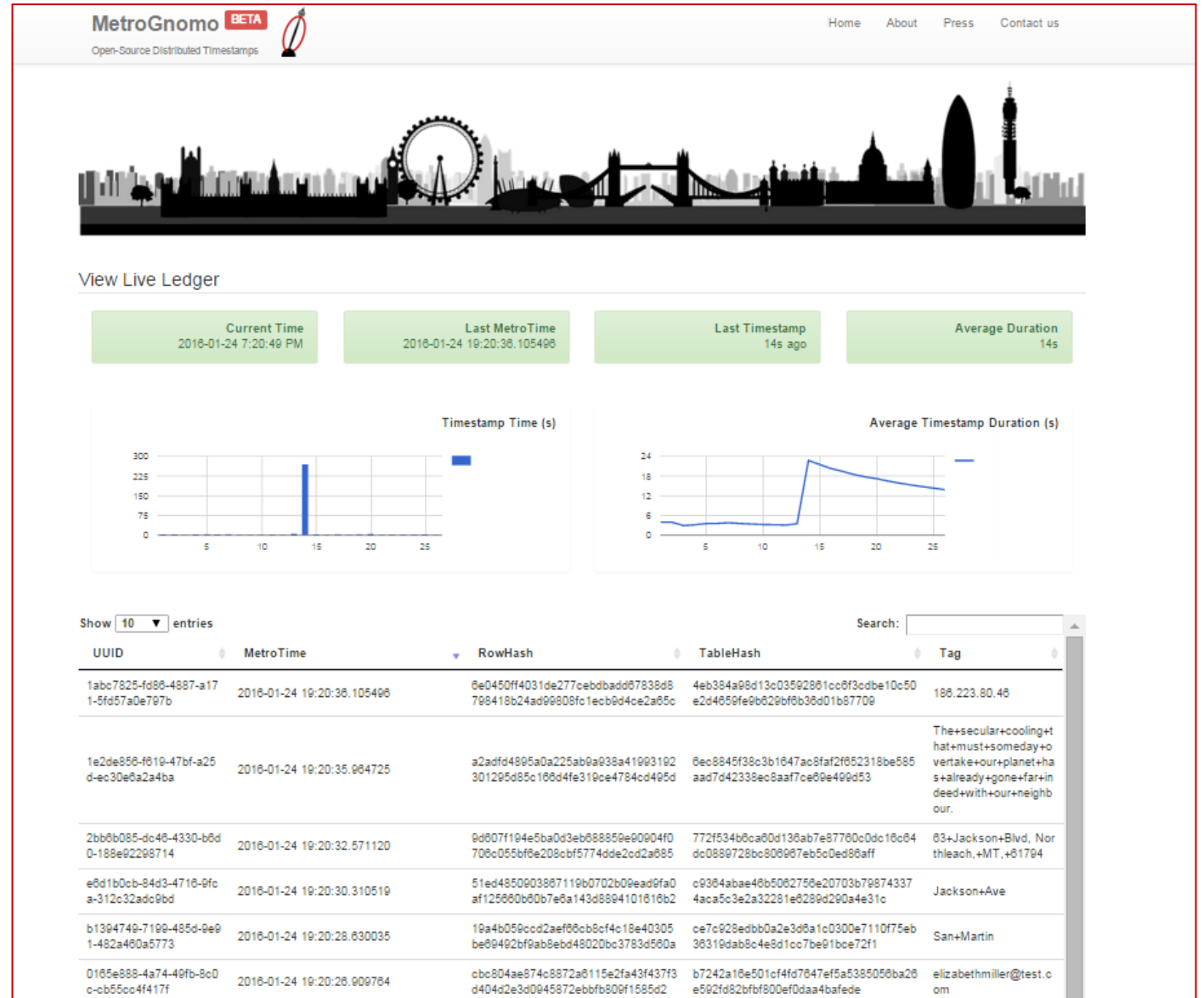
# Boring! What's An Exciting One Look Like?



MetroGnomo BETA  
Open-Source Distributed Timestamps

Stamp #! Check Stamp Retrieve File  
Register View Live Ledger Host Receiver

Obtaining Proof Of Existence



MetroGnomo BETA  
Open-Source Distributed Timestamps

Home About Press Contact us

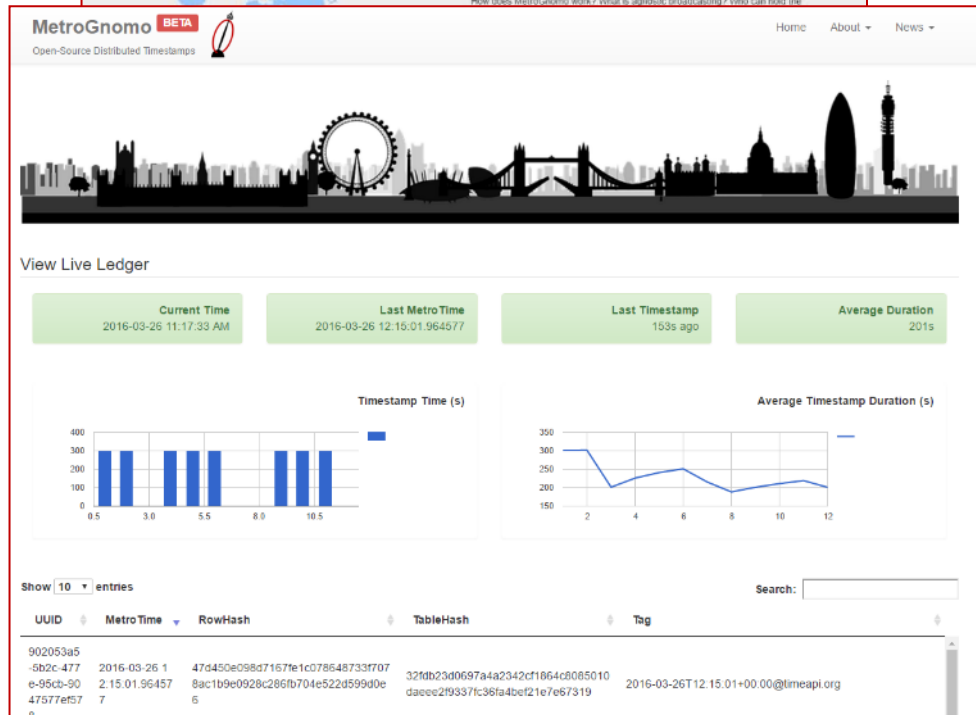
### View Live Ledger

Current Time: 2016-01-24 7:20:49 PM  
Last MetroTime: 2016-01-24 19:20:36.105496  
Last Timestamp: 14s ago  
Average Duration: 14s

Timestamp Time (s) and Average Timestamp Duration (s) graphs.

Show 10 entries

UUID	MetroTime	RowHash	TableHash	Tag
1abc7825-fd88-4887-a171-5fd57a0e797b	2016-01-24 19:20:36.105496	6e0450ff4031de277cebdadd87838d8798418b2d4ad99808f1ecb8d4ce2a85c	4eb384a98d13c03592861cc8f3c0d8e10c50e2d4859fe9b829bf6b36d01b87709	188.223.80.48
1e2de858-f619-47bf-a25d-c30e8a2a4ba	2016-01-24 19:20:35.984725	a2adf4895a0a225ab9a938a41993192301295d85c106d4fe319ce4784cd495d	6ec8845f38c3b1647ac8faf2f652318be585aad7d42338ec8aaf7ce09e499d53	The+secular+cooling+hat+must+someday+overtake+our+planet+has+already+gone+far+in+deed+with+our+neighbor.
2bb8b085-dc48-4330-b6d0-188e92298714	2016-01-24 19:20:32.671120	9d907f104e5ba0d3eb888859e09004f0708c055bf8e208cbf5774dde2cd2a885	772f534b8ca80d136ab7e87780c0dc16c84dc0889728bc808987eb5c0ed86aff	83+Jackson+Blvd, Northleach,+MT,+81784
e8d1b0cb-84d3-4716-9fca-312c32adc9bd	2016-01-24 19:20:30.310519	51ed4850903887119b0702b09ead9fa0af125860b90b7e8a143d8894101616b2	c9384abae46b5082758e20703b798743374aca5c3e2a32281e8289d290a4e31c	Jackson+Ave
b1394749-7199-485d-9e91-482a460a5773	2016-01-24 19:20:28.630035	19a4b059ccd2aef86cbcf4c18e40305be9492bf9ab8ebd48020bc3783d580a	ce7c928edbb0a2e3d8a1c0300e7110775eb36319dab8c4e8d1cc7be91bce72f1	San+Martin
0165e888-4a74-49fb-9c0c-cb55cc4f417f	2016-01-24 19:20:26.909784	cbc804ae874c8872a6115e2fa43f437f3d404d2e3d0945872ebbf809f1585d2	b7242a16e501cf4fd7847ef5a5385058ba28e592fd82bfbf800ef0daa4bafede	elizabethmiller@test.com



MetroGnomo BETA  
Open-Source Distributed Timestamps

Home About News

### View Live Ledger

Current Time: 2016-03-26 11:17:33 AM  
Last MetroTime: 2016-03-26 12:15:01.964577  
Last Timestamp: 153s ago  
Average Duration: 201s

Timestamp Time (s) and Average Timestamp Duration (s) graphs.

Show 10 entries

UUID	MetroTime	RowHash	TableHash	Tag
90203a5-5b2c-477e-95cb-9047577ef57	2016-03-26 2:15:01.96457	479450e098d7167fe1c0786487337078ac1b9e0928c286fb704e522d599d0c6	321db23d0697a4a2342cf1664c0885010da0cc2f93371c38fa4bcf21e7e67319	2016-03-26T12:15:01+00:00@timeapi.org

# Boring!!! What's Another Look Like?



[About](#) - 
 [Stats](#) - 
 [Case Studies](#) - 
 [Products](#) - 
 [The Mutual](#)

Last Geo Timestamps (UTC)  
2022-03-17 17:26:57.164275

Total Geo Timestamps  
**6132**  
in last 24 Hours

Total Cities  
**1092**  
in last 24 Hours

Total Countries  
**116**  
in last 24 Hours

Geo Timestamp Rate  
**0.0710**  
per second

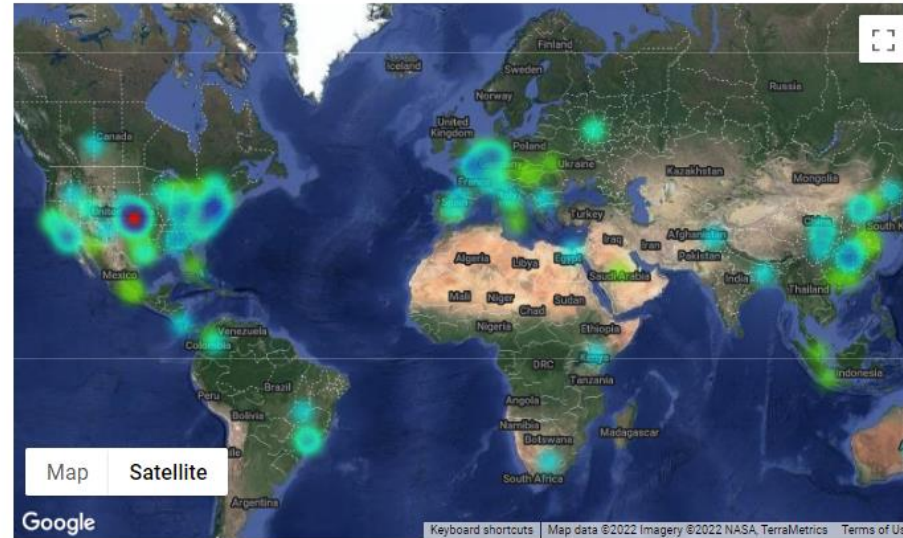
## Timestamps Location

Last Stamp Country  
**Indonesia**

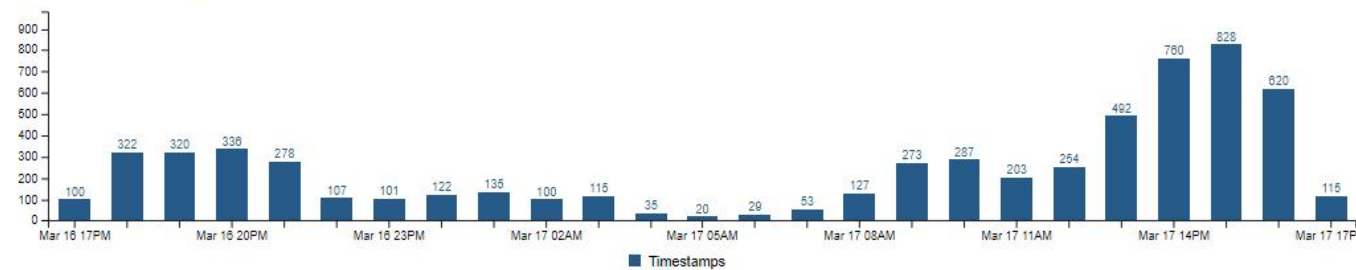
Last Stamp City  
**N/A**

Top Countries

<b>United States</b>	42.45%
<b>China</b>	9.57%
<b>Japan</b>	5.41%
<b>United Kingdom</b>	3.64%
<b>Germany</b>	3.44%



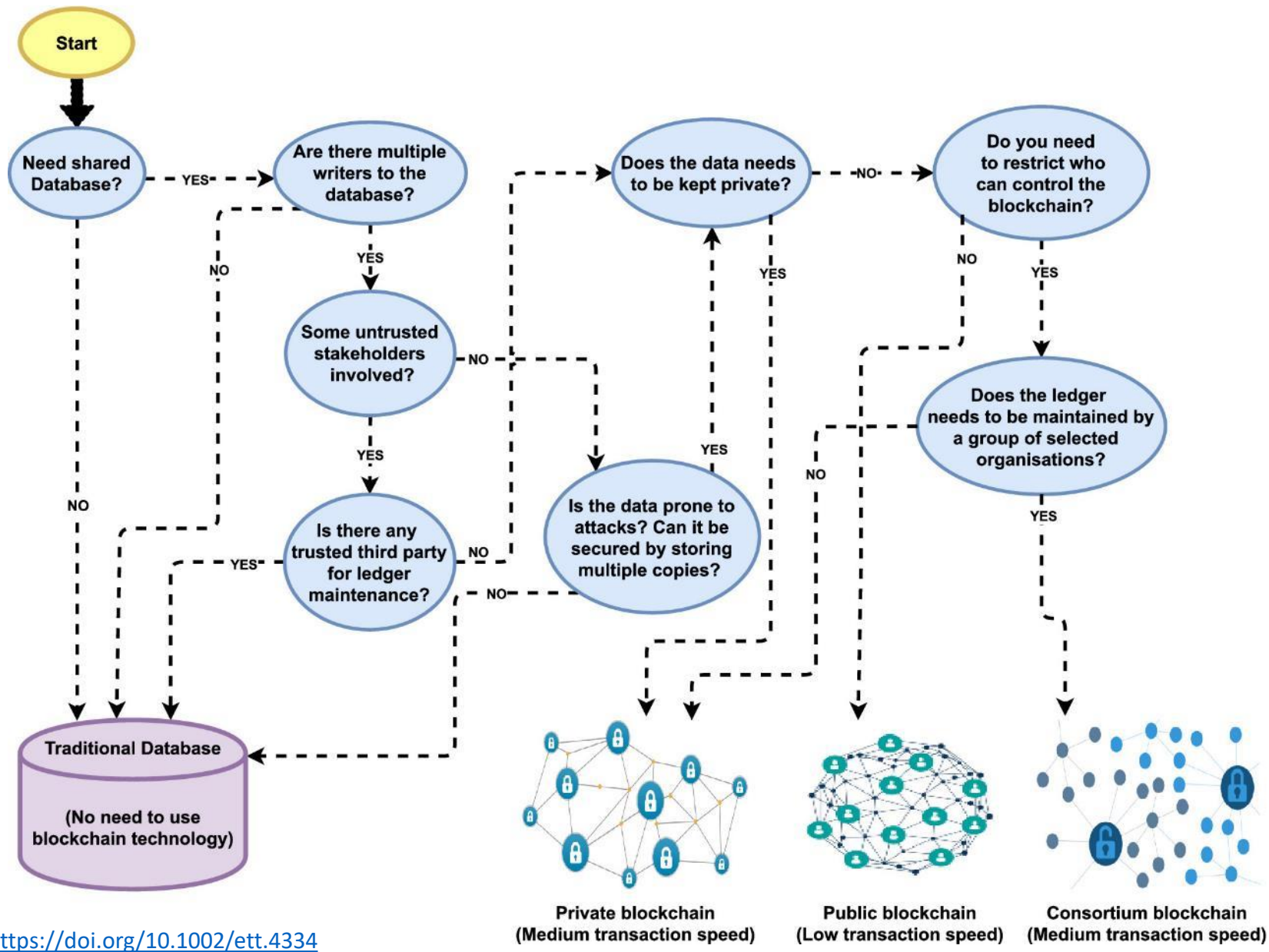
## Activities in last 24 hours



# Possibly Distributively Ledgerable

Financial Instruments, Records, Models		Public Records		Private, Semi-Private/Semi-Public Records		Physical Keys, Intellectual Property, Other Records	
Currencies	Derivatives	Land & Property Titles	Vehicle Registries	Contracts	ID	Home Key	Hotel Key
Commodities	Insurance Policies	Shipping Registries	Satellite Registries	Signature	Will	Office Key	Car Key
Trading Records	Private and Public Equities	Business License	Business Ownership Records	Trust	Escrow	Deposit Box Key	Mail Box Key
Certificates of Deposit	Bonds	Incorporation / Dissolution Records	Regulatory Records	Other Classifiable Data	High School / University Degrees	Internet Of Things	Copyrights & Patents
Voting Rights (Financial Services)	Credit Data	Criminal Records	Passport	Professional Qualifications	Certifications	Licenses	Digital Rights Management
Collateral Management	Client Monies Segregation	Birth / Death Certificates	Voting ID	Human Resources Records	Medical Records	Trademarks	Proof Of Authenticity / Authorship
Mortgage / Loan Records	Crowd-Funding	Health & Safety Inspections	Tax Returns	Accounting Records	Business Transaction Records	Cultural Events	Historical Events
P2P Lending	Microfinance	Building & Other Types Of Permits	Court Records	Locational Data	Genome & DNA	Documentaries	Big Data
Account Portability	Airmiles / Corporate Tokens	Government / Listed Companies	Accounts & Annual Reports	Arbitration	Genealogy Trees	SIM Cards	Archives

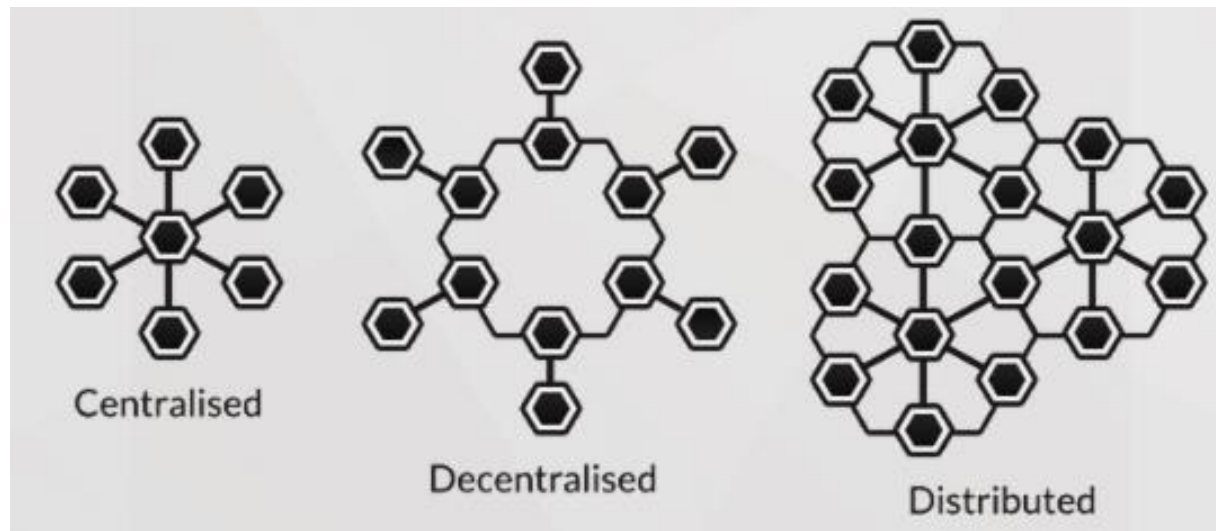
# Where Should I Use This Smart Ledger Stuff?



# Reducing Natural Monopolies

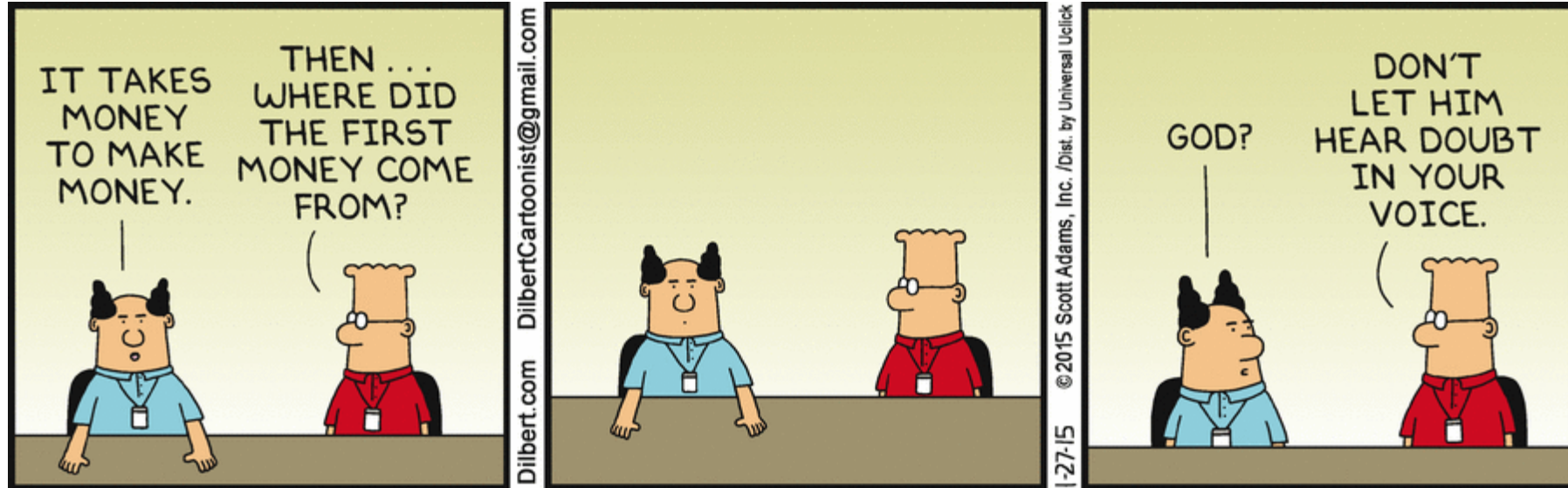
- ? Validate – “a trust model for timestamping.”
- ✓ Safeguard – “a set of rules for updating state via blocks.”
- ✓ Preserve – “a shared state.”

## *Immutable, Persistent & Pervasive*

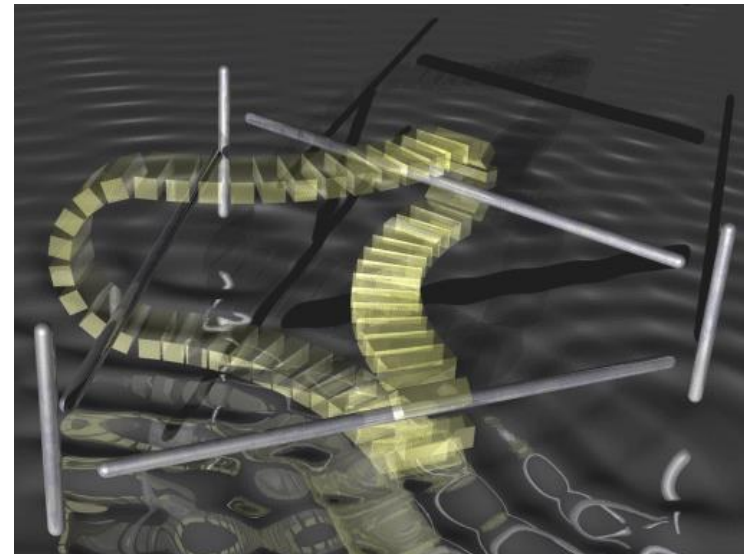




# The Study Of Money Is The Root Of Much Madness



[www.dilbert.com, Thursday, 27 January 2015]



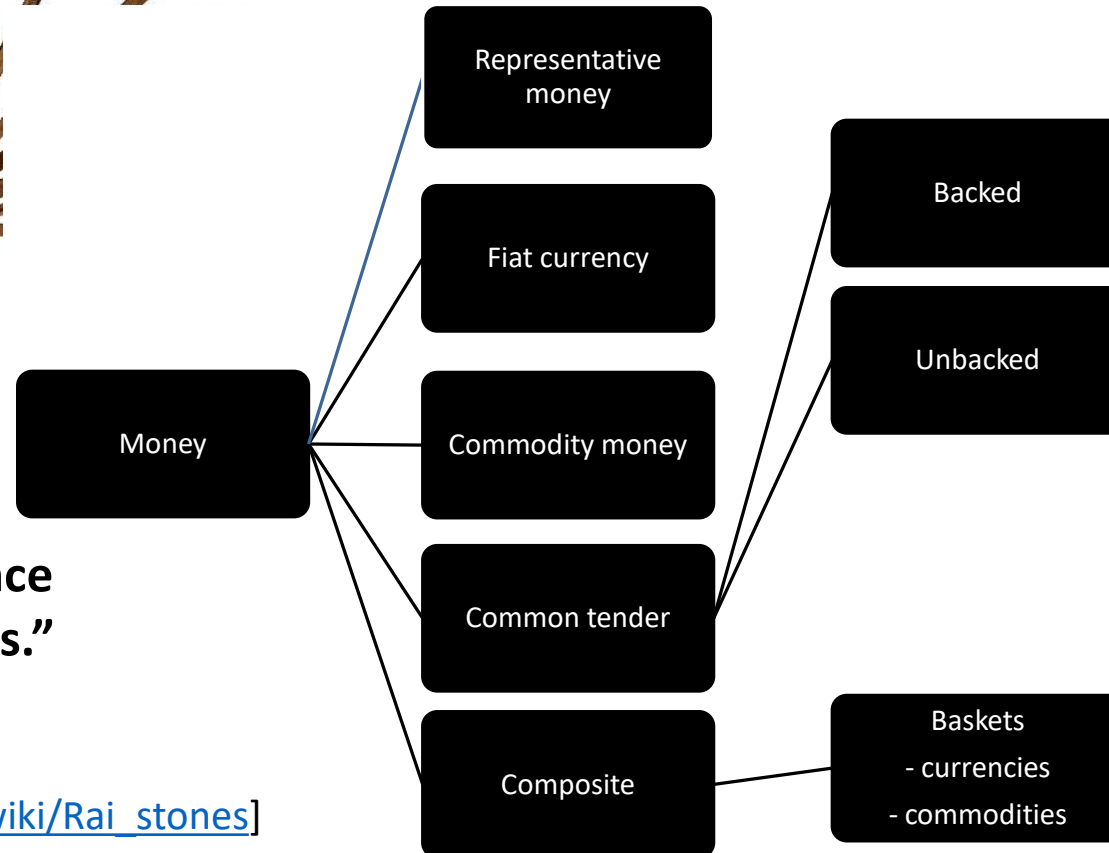
[<http://illusionsetc.blogspot.com/2005/08/moving-mobius-strip.html>]

# Money As Technology



**“Money is a technology communities use to trade debts across space and time.”**

**“Tokens of indebtedness are social desires frozen at a point in time – tokens depend on the future persistence of the community and its values.”**



[SOURCE: [https://en.wikipedia.org/wiki/Rai\\_stones](https://en.wikipedia.org/wiki/Rai_stones)]

# Bitcoin Primer

## How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

### WALLETS AND ADDRESSES



Bob and Alice both have Bitcoin "wallets" on their computers.



Wallets are files that provide access to multiple Bitcoin addresses.



An address is a string of letters and numbers, such as 1HULMwZEPkJECh43BakLLybLCWrfDpN.



Bob creates a new Bitcoin address for Alice to send her payment to.

### CREATING A NEW ADDRESS



Each address has its own balance of bitcoins.

### SUBMITTING A PAYMENT



Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.

Private key



Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.



Public key

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

### Public Key Cryptography 101

When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

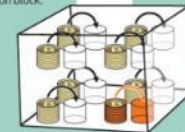
It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

Gary, Garth, and Glenn are Bitcoin miners.

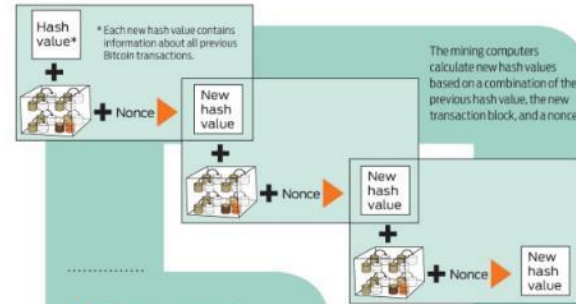


### VERIFYING THE TRANSACTION

The miners' computers are set up to calculate cryptographic hash functions.



Their computers bundle the transactions of the past 10 minutes into a new "transaction block."



### Cryptographic Hashes

Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

- The root of all evil: 6d0a1899086a... (56 more characters)
- The root of all evil: 485c6be46dde...
- The root of all evil: b8db7ee98392...

### Nonces

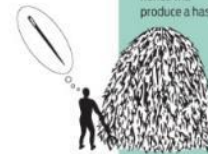
To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

The root of all evil ???

0000 0000  
0000 ...

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash



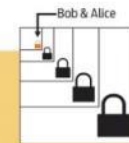
value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.



### TRANSACTION VERIFIED

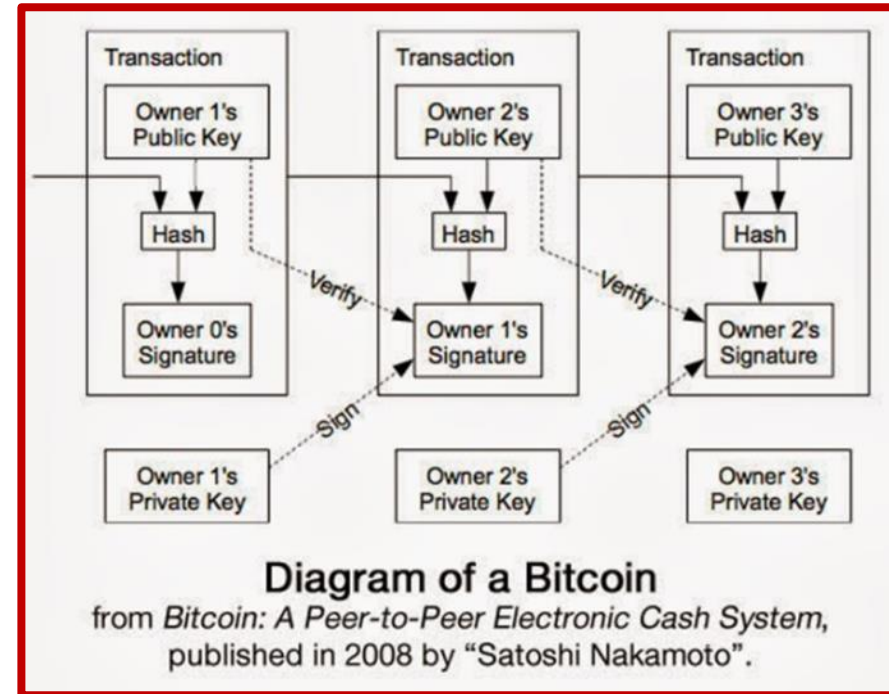
As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.



# Ledgers: Look Beneath The Coins

“...  
the potential impact of the distributed ledger may be much broader than on payment systems alone. The majority of financial assets — such as loans, bonds, stocks and derivatives — now exist only in electronic form, meaning that the financial system itself is already simply a set of digital records.”

*Bank of England, Quarterly Bulletin (2014, Q3)*



“In distributed ledger technology, we may be witnessing one of those potential explosions of creative potential that catalyse exceptional levels of innovation.”

Matthew Hancock & Ed Vaizey (January 2016)

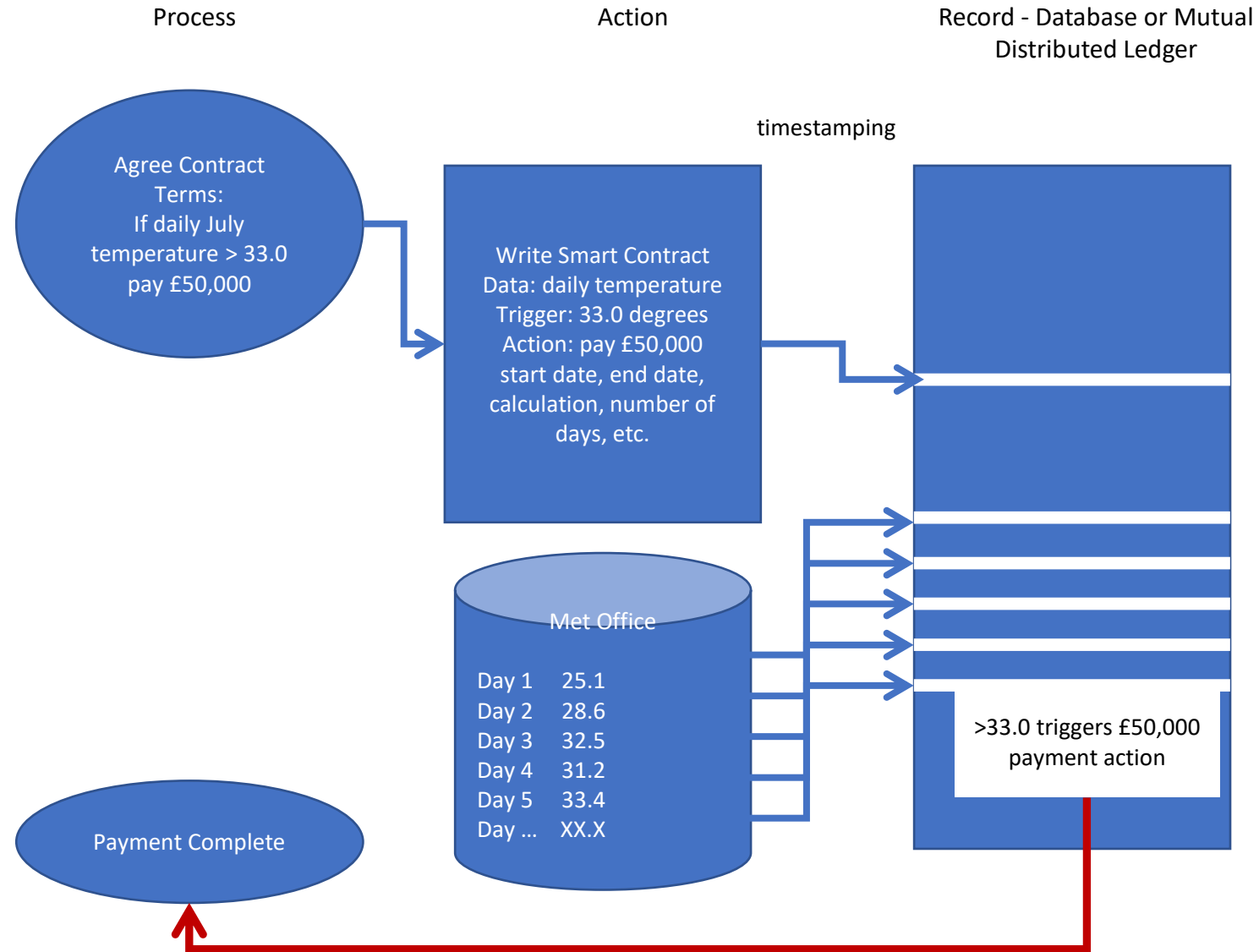
# Smart Contract - 1986



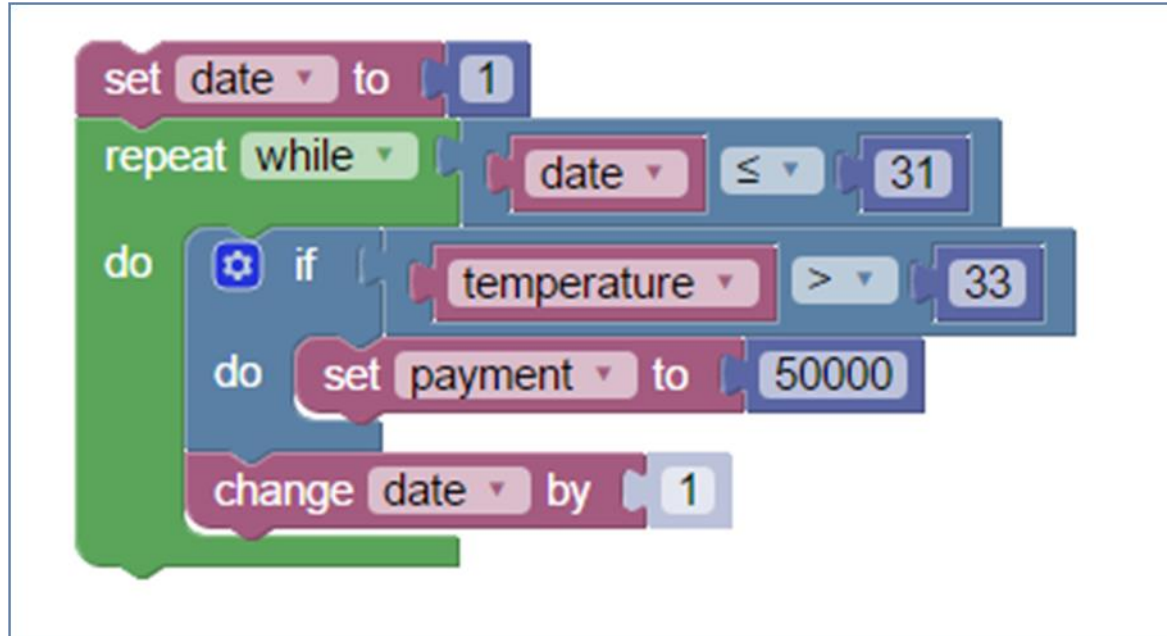
4-01	\$	8,336.36	\$	
5-01	\$	8,130.02	\$	
6-01	\$	7,922.69	\$	246.56
7-01	\$	7,714.36	\$	
8-01	\$	7,505.02	\$	246.56
9-01	\$	7,294.68	\$	246.56
10-01	\$	7,083.31	\$	246.56



# Weather Smart Contract Example



# Contract As Code



```
Language: JavaScript ▼  
  
var Count, date, payment, tempera  
  
date = 1;  
while (date <= 31) {  
  if (temperature > 33) {  
    payment = 50000;  
  }  
  date = (typeof date == 'number'  
}
```

# Follower Syndicate In Code

```
set % underwriting to 0
set # Insurers >= 7% to 0
if A u/w% ≥ 7
do change # Insurers >= 7% by 1
if B u/w% ≥ 7
do change # Insurers >= 7% by 1
if C u/w% ≥ 7
do change # Insurers >= 7% by 1
set Total u/w% to A u/w% + B u/w% + C
if Total u/w% ≥ 20
do if # Insurers >= 7% ≥ 2
do set % underwriting to Total u/w% × 0.03
```

Language: Python

```
from numbers import Number

__Insurers__3E__7_25 = None
__25_underwriting = None
A_u_w_25 = None
B_u_w_25 = None
C_u_w_25 = None
Count = None
D_u_w_25 = None
Total_u_w_25 = None

__25_underwriting = 0
__Insurers__3E__7_25 = 0
if A_u_w_25 >= 7:
    __Insurers__3E__7_25 = (__Insur
if B_u_w_25 >= 7:
    __Insurers__3E__7_25 = (__Insur
if C_u_w_25 >= 7:
    __Insurers__3E__7_25 = (__Insur
Total_u_w_25 = (A_u_w_25 + B_u_w_
if Total_u_w_25 >= 20:
    if __Insurers__3E__7_25 >= 2:
        __25_underwriting = Total_u_w_
7
if false:
    pass
```

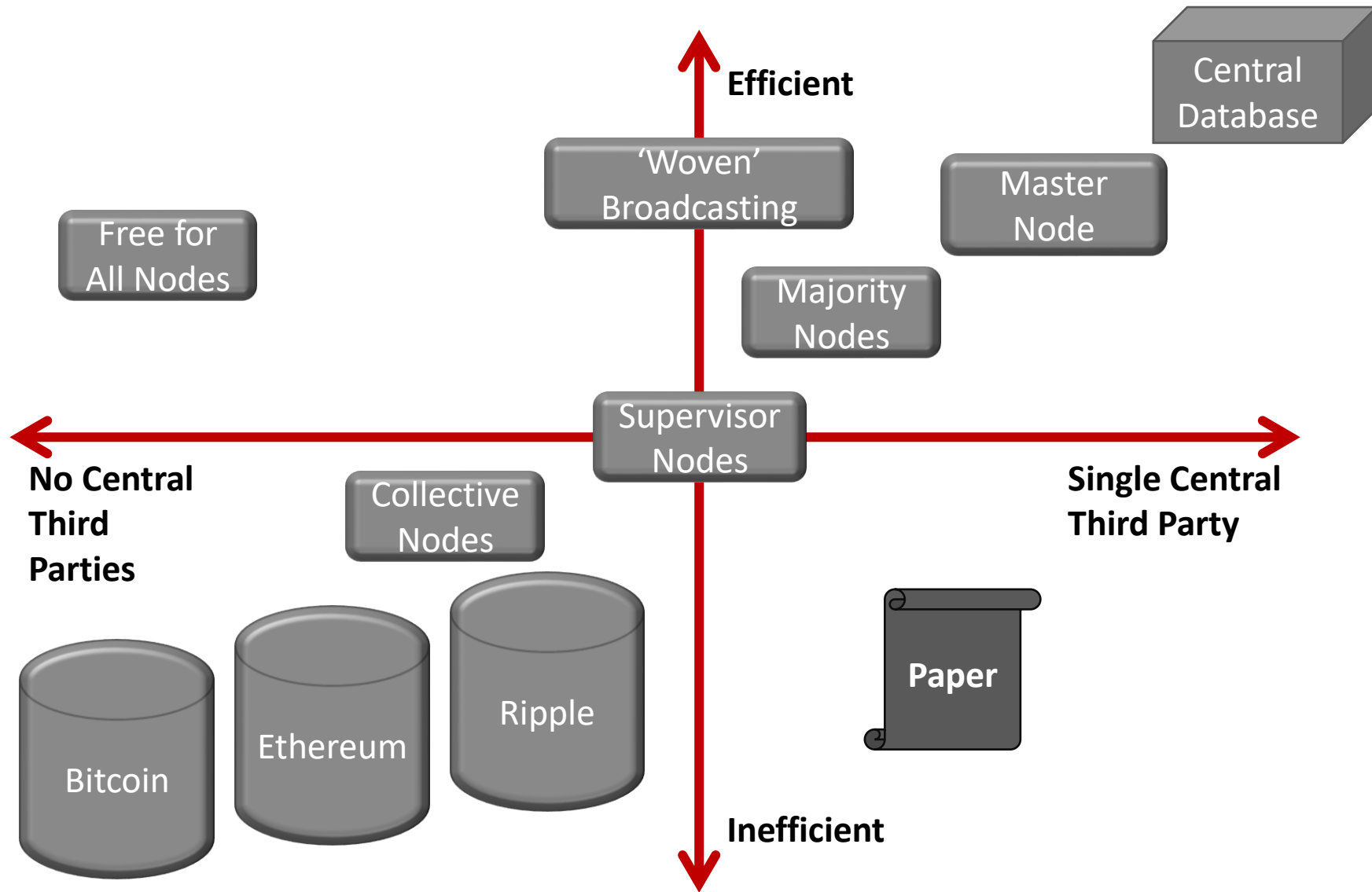


# Terminology Evolving

- **Ledger:** a record of transactions.
- **Distributed:** divided among several or many, in multiple locations
- **Mutual:** shared in common or owned by a community.
- **Mutual distributed ledger (MDL):** a record of transactions shared in common and stored in multiple locations.
- **Mutual distributed ledger technology:** a technology that provides an immutable record of transactions shared in common and stored in multiple locations.
- **Node:** a dedicated server that stores and rebroadcasts validated blocks and transactions across an MDL network.
- **Blockchain:** “a transaction database shared by all nodes participating in a system based on the Bitcoin protocol.”
- **Smart ledger:** MDL with embedded, executable code



# Mistrust Costs Coins



## People Who Need People...

There will be dispute resolution problems that only humans can solve:

- Ricardian contracts and 'smart' contracts – data sources ('oracles') – create real coding issues
- Time – 'short and dumb' well before 'long and smart'
- Agreements more complex than payments – identity over time, promises over time, value over time, *force majeure*, volatility
- Synthetic jurisdictions
- Problems with enforcement



# Dispute Resolution Processes

Characteristics	<i>Negotiation</i>	<i>Mediation</i>	<i>Arbitration</i>	<i>Adjudication</i>
<b>Outcome</b>	Mutually acceptable agreement sought	Mutually acceptable agreement sought	Sometimes principled decision supported by reasoned opinion; sometimes compromise without opinion	Principled decision supported by reasoned opinion; rarely compromise without opinion
<b>Orientation</b>	Future-oriented	Future-oriented	Past-oriented	Past-oriented
<b>Private/public</b>	Private	Private	Private, unless judicial review sought	Public

## What's A Poor Arbitrator's Opportunity?

- Legally complicated and expensive
- Internationally expensive
- Mostly about commercial contracting
- Mostly about unforeseen events



# Mattereum restores trust with **warranted specifications**

## Physical Asset



## Mattereum Asset Passport

provides buyers with surety that is independent of the vendor



Digital Smart Contract



Warranties



OEM / Experts



Insurers



Legal Process

- ✓ Precise specification
- ✓ Parametric search by specification
- ✓ Asset inventory with no listing fees
- ✓ Automated and on-chain transaction
- ✓ Powerful knowledge graph

① Digital smart “Ricardian” contract linked to the object purchase

② OEM or independent experts issue warranties with precisely defined claims, backed by insurance

③ Claims enforceable in 160+ jurisdictions through arbitration without additional customer burden

*Trust in the seller is replaced by certainty around the value of the claims attached to the item being transacted*

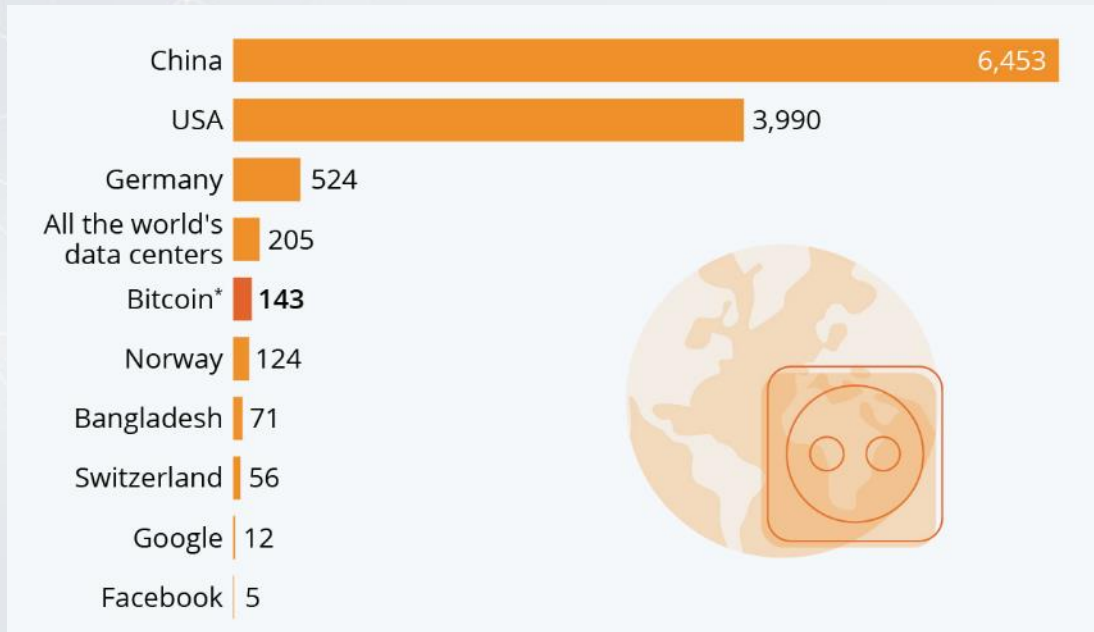
# Enables trustable trades for delivery and vaulted items



# Using the blockchain – the right way

## Bitcoin - the new “coal”

Annual energy consumption (TWh)



## AVALANCHE

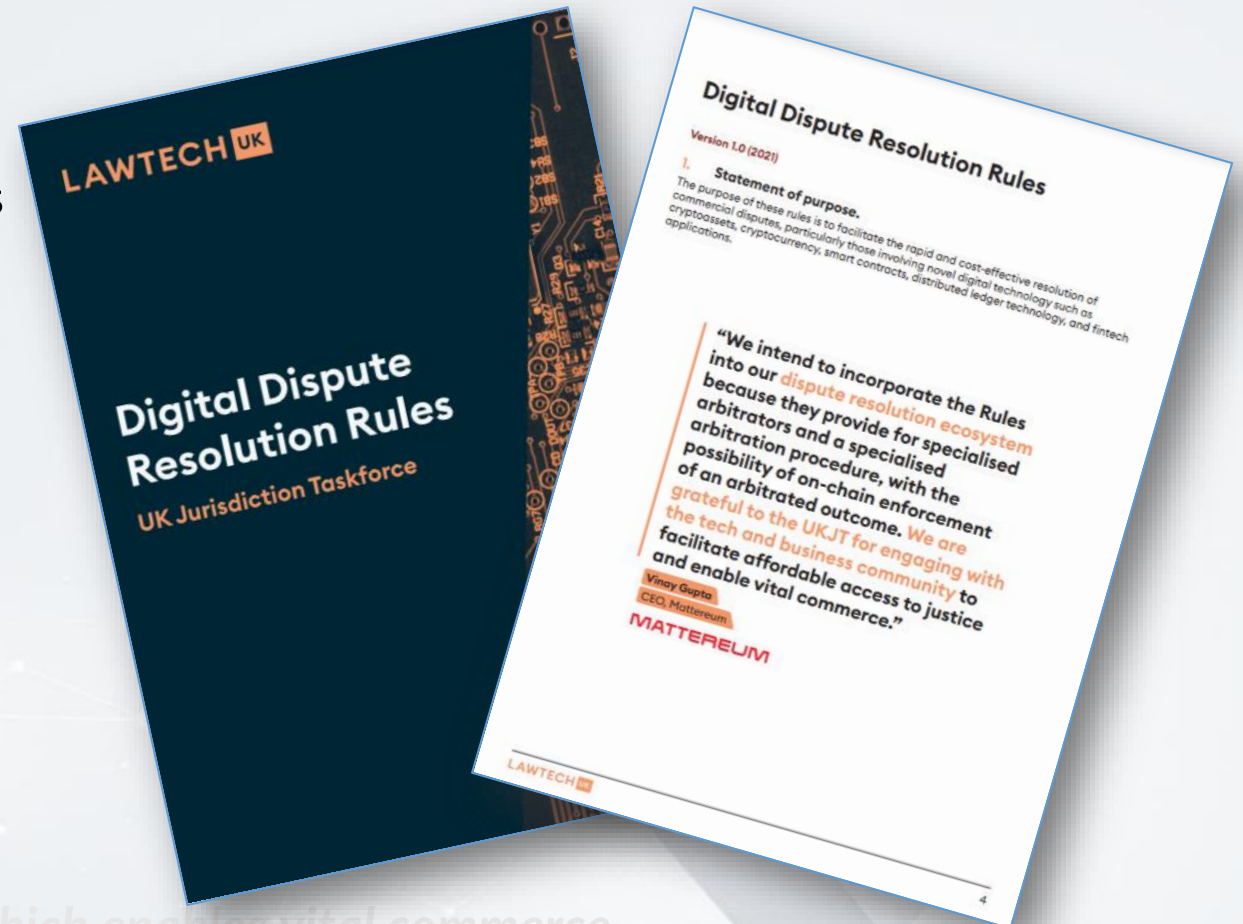
- ✓ Open, programmable smart contracts platform for decentralized applications.
- ✓ Fast
- ✓ High throughput
- ✓ Interoperable with other blockchains
- ✓ Proof-of-stake
- ✓ Low energy consumption
- ✓ Low gas cost
- ✓ Fully-offset

*Our own use of blockchain technology is fast, lightweight, low cost and full sustainable*



# Digital + legal innovation: *assured global enforceability*

- Mattereum smart contracts are legally enforceable in **160+ jurisdictions**
- We have worked closely with legal professionals and members of the judiciary to build a fair and **just arbitration ecosystem**
- **Cooperation** with the UK Jurisdiction Taskforce overseen by the Master of the Rolls
  - new **Digital Dispute Resolution Rules** designed to facilitate digital commerce
- Mattereum's legal counsel include global law firm **Sidely Austin** and the award-winning **Gunner Cooke**



*Affordable justice which enables vital commerce*

# UK Jurisdiction Taskforce

## Foreword

In November 2019, the UK Jurisdiction Taskforce published its [Legal Statement on the Status of Cryptoassets and Smart Contracts](#). The Legal Statement expressed the view that cryptoassets were property and smart contracts were contracts under English law, and has been very well received in many jurisdictions.

The UK Jurisdiction Taskforce is now publishing its Digital Dispute Resolution Rules to be used for and incorporated into on-chain digital relationships and smart contracts. They are ground-breaking in that they allow for:

- Arbitral or expert dispute resolution in very short periods
- Arbitrators to implement decisions directly on-chain using a private key
- Optional anonymity of the parties

The **Digital Dispute Resolution Rules** have been drafted after extensive public and private consultation with lawyers, technical experts and financial services and commercial parties.

I am confident that the **Digital Dispute Resolution Rules** will be incorporated into many types of digital transaction going forward. The UK Jurisdiction Taskforce will keep a close watch on how the Digital Dispute Resolution Rules are used, and will aim to consider whether experience suggests they need revision within the coming year.

I am extremely grateful to the sub-committee, which has worked so hard to prepare these Rules (Lawrence Akka QC, David Quest QC, Dorothy Livingston, Anne Rose, David McIlwaine, Richard Hay and Rory Conway).



**Sir Geoffrey Vos**  
Master of the Rolls



# Mattereum Moves

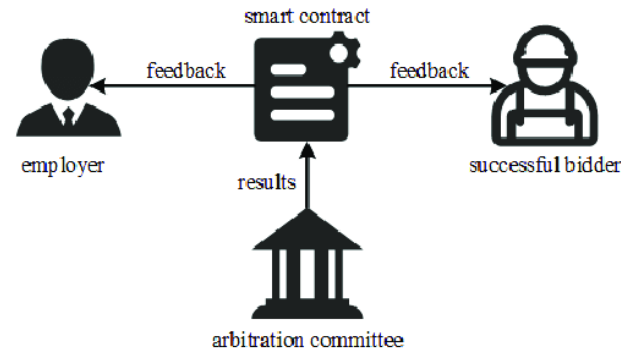
“We intend to incorporate the Rules into our **dispute resolution ecosystem** because they provide for specialised arbitrators and a specialised arbitration procedure, with the possibility of on-chain enforcement of an arbitrated outcome. **We are grateful to the UKJT for engaging with the tech and business community to facilitate affordable access to justice and enable vital commerce.**”

Vinay Gupta

CEO, Mattereum

**MATTEREUM**

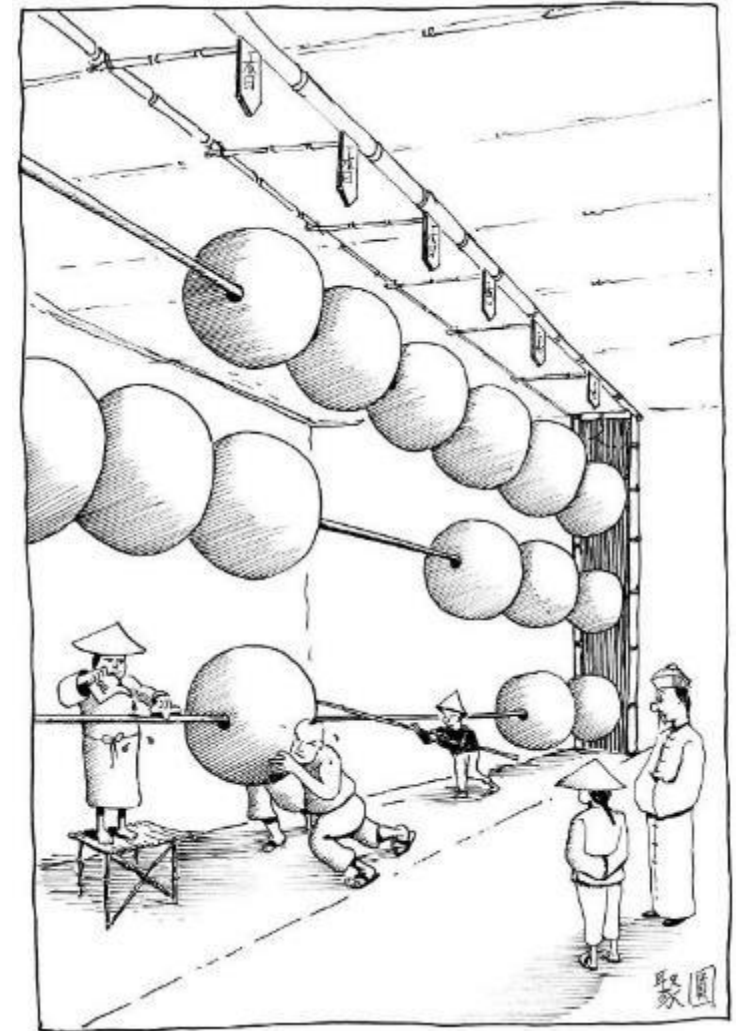
# Arbitrate The Arbitrators?



- Traditional arbitration - two banks enter into a smart contract to sell securities via a clearing system, backed up by a written contract with an arbitration clause. A dispute arises. The parties agree to arbitrate. The clearing system allocates an arbitrator experienced in smart contract disputes. Each bank nominates that arbitrator and the smart contract automatically empowers that person to retransfer the securities and/or the purchase price. On delivering the award after arbitration, the arbitrator makes the transfer.
- Smart ledger arbitration: two individuals in different countries enter into a smart contract to exchange currencies. One party registers a dispute with the smart contract which automatically raises a bid for arbitrators with a pool of smart contract arbitrators – the first arbitrator with a high enough reputation score to accept the bid is allocated as the delegate. The individuals email their submissions to the smart contract which forwards them to the appointed arbitrator. The arbitrator's response is emailed back to the individuals via the contract and any transfer or retransfer of currency made by the smart contract.

## What's A Poor Arbitrator To Do?

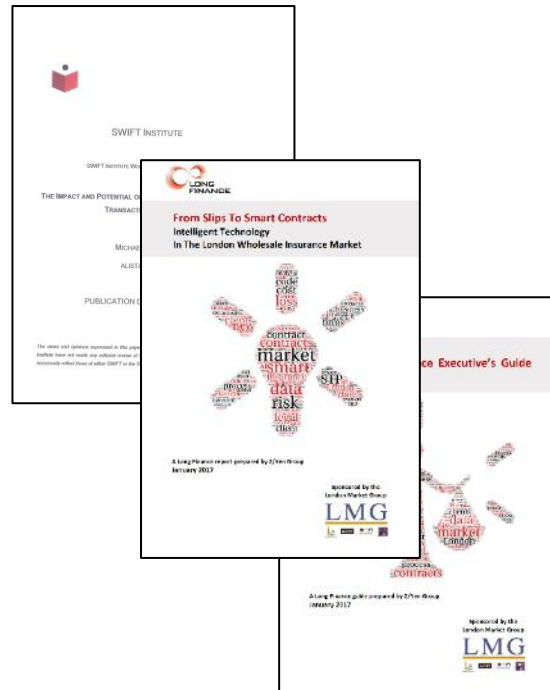
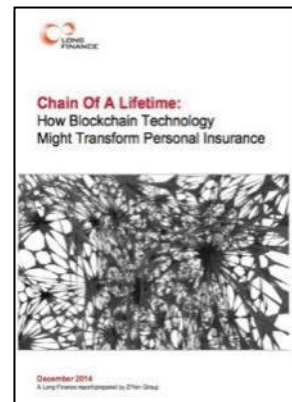
- 'Up' your skills base
- Promotion of the 'open door' to the arbitration community – bulletins, events, articles
- Suggest T&C's that specify delegation to an arbitrator and legal right to arbitrate
- Create a pool of arbitrators willing and able to respond to this arbitration mechanism



**“Get a big picture grip on the details.”**  
**Chao Kli Ning**

# The Long-Term?

Theme	Service	Question
Trust	Identities/Assets	Authentication
Space	Transactions	Services
Time	Debts	Value-added
Mutuality	Contracts	Common-wealth



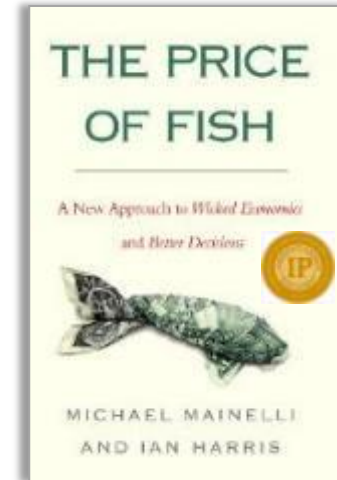
# Comments, Observations, Questions, Answers (?)



# When Would We Know Commerce Is Working?



**“Get a big picture grip on the details.”**  
*Chao Kli Ning*



**Thank you!**





# Beyond The Bandwagon – Blockchain Is So Passé

