Transactional Immunity WHITEPAPER: in re US6370629

Transactional Immunity for uses of eCurrencies and their Consensus Algorithms, Hashing Software, Wallet Operations, and their uses of US6370629 Methods.

Todd S. Glassey, Principal Inventor US6370629,
Sole Inventor of Location Based Service technologies
v 1.0 - 18.10.2018

Table of Contents

Transactional Immunity WHITEPAPER: in re US6370629

Transactional Immunity WHITEPAPER: in re US6370629

Abstract

I am NOT a Lawyer, so consult your own on this. This white paper outlines the “Uses of US6370629 Methods in eCurrency Generation, Processing, Posting, and Transactions” of those eCurrencies available today and the various Legal Implications of those actions based on the US6370629 Settlement, the Ruling of the US DC Court in 14-03629/WHA and its appeals (Ninth Circuit 14-17574 and DC Circuit 15-01326) as well as actions in subsequent US Federal Court matters and US Department of Justice Policies towards these eCurrencies and their uses in the US and abroad.

It also speaks to the transactional immunity issued by the US DOJ through its continual and repeated refusal to prosecute any party illegally using US6370629 for anything, and the US Courts refusal to prosecute any party as well for the same illegal uses of US6370629 methods and their hundreds of derivatives.

This Document

This Document provides a basis as a Defense Tool in prosecutions where Money Laundering or related claims are charged in the US, AU, BR, CA, EU, UK, KO, JP, and ZA jurisdictions today.

Published in English specifically for its use in US, Great Britain and other English Speaking Nations (Denmark)

This document is intentionally written in English to apply to US, Canadian, Australian, EU, South African, Great Britain, Scotland, Wales, Ireland (ROI and UK’s Norther Ireland), as well as all other English Speaking Nations of the Earth.

A Russian and Chinese instance is available separately for use in Russia and Russian and Chinese Speaking Nations as well.

Its Purpose – a one stop document for Lawyers and Technologists pertaining to US6370629 Transactional Immunity

This document is a direct analysis of Legal Implications of Nations formally granting Transactional Immunity of the numerous illegal uses of US6370629 methods inside various eCurrency Systems.

Its purpose is to provide a basis of Claim Construction in submissions to various legal authorities in eliminating or reducing criminal antitrust charges based therein against parties using these IP’s in their alleged financial crime actions.

As such it is intended to be a defense tool properly documenting the transcendental form of Transactional Judicial Immunity which has been applied to any and all uses of these Intellectual

Transactional Immunity WHITEPAPER: in re US6370629

Properties outside the terms of the US6370629 Settlement by the US Department of Justice and related entities.

The Document Sections

This document is split into a Technologies Sections and then a Legal Implications Section.

For Lawyers: The Law and Legal Implications Section

The Legal Implications Section defines just that and overviews virtually all of the key aspects we believe, related to financial systems processing in eCurrency and Banking today. The Transactional Immunity areas are at the end and beginning of the section.

For Technologists: The Technologies

The Technologies Section is provided to meet the burden of proof requirement for the uses of US6370629 inside eCurrency Systems, and show specifically where in Mining, Consensus Algorithm Processing, and in eCurrency Wallet and Exchange Service processing, US6370629 Methods are used.

For Lawyers: The Excluded areas of Enforcement Review

No focus on Weapons Systems which also illegally use these Intellectual Properties is provided in this document.

Nor is any Rome Statute standing issues pertaining to the conversion (appropriation of the IP) under Rome Statute §8(2)(b)(iv) and related statute clauses.

Section 1 – For Lawyers

The Legal Implications

This section speaks to the original conversion frauds, and their subsequence legal implication in prosecuting legal claims, specifically criminal ones, but civil ones as well, pertaining to the uses of US6370629 protected methods in systems used in criminal manners. It also speaks to the continuous refusal to prosecute any party for any illegal uses of US6370629 or its derivatives, both through the US DOJ and through a Judicially Initiated Prosecution demanded by Plaintiffs in USDC 14-03629/WHA. It is these actions which created the De-facto Transactional Immunity per the terms and precedents set forth herein.

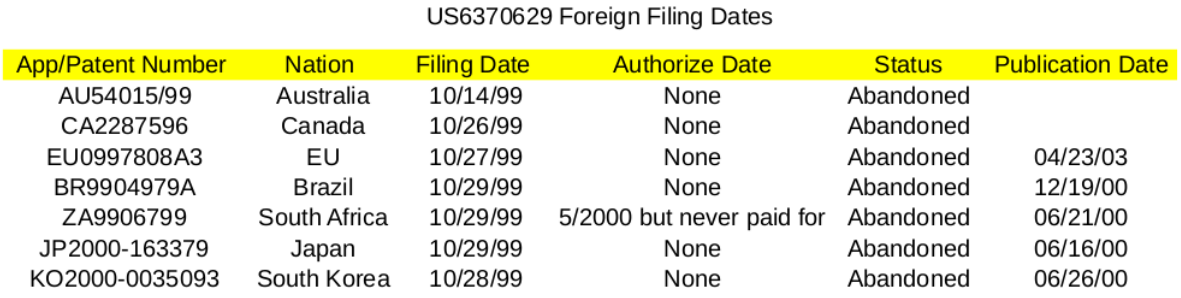
What is this matter about? LOCATION BASED SERVICES

This matter pertains to the Frauds the US and related Governments used to convert ownership of the Location Based Service (“LBS”) component of US6370629. It is those LBS components which are today inside every commercial software everywhere, and especially used in a number of applications from eCurrencies and Banking to Weapons and Energy Control Systems.

It also pertains to the concept of transactional immunity which the US Government created both through its DOJ and through its Court System for blocking any and all prosecutions for the conversion and use of US6370629 in any form in any number of software, banking and weapons systems in use globally today.

Government protected frauds create a Transactional Immunity for all like uses

Because the US, British, EU, Canadian, Brazilian, Australian, South African, South Korean, Japanese and other Governments directly give US and local Companies legal immunity from any unlawful uses of US6370629 methods in their nations, because the seven Jurisdictions have given those parties who filed and abandoned the seven illegally filed instances, full Judicial Criminal Immunity, and because those Nations refused to revive and properly assign the ownership of those patents to their rightful owners, they have acted in a manner “To first commit a criminal antitrust matter, appropriate US Citizens Intellectual Properties and then convey full interest to their own Public Domain”, a direct fraud and violation of United Nations statutes for Human Rights. Thus also violating “The Rome Statutes Section §8(2)(b)(iv) Appropriation of Property clauses”.



US6370629 Foreign Filing Dates

App/Patent Number	Nation	Filing Date	Authorize Date	Status	Publication Date
AU54015/99	Australia	10/14/99	None	Abandoned	
CA2287596	Canada	10/26/99	None	Abandoned	
EU0997808A3	EU	10/27/99	None	Abandoned	04/23/03
BR9904979A	Brazil	10/29/99	None	Abandoned	12/19/00
ZA9906799	South Africa	10/29/99	5/2000 but never paid for	Abandoned	06/21/00
JP2000-163379	Japan	10/29/99	None	Abandoned	06/16/00
KO2000-0035093	South Korea	10/28/99	None	Abandoned	06/26/00

The USDC 14-03629/WHA ruling

All uses of US6370629 are controlled by a US District Court ruling from 14-03629/WHA which perfected the terms of the Settlement.

The Ruling of the US DC Court in 14-03629/WHA was affirmed and as such cross perfected in two separate Circuits of the US Courts, the Ninth and DC Circuits. These were done in Appeals number 14-17574 for the Ninth Circuit, and 15-01326 for the DC Circuit.

Obtaining a Published Ruling effect by Cross Filing the appeal before the DC Circuit

The net effect of this unique Dual Appeal Process was to bind the US Government and the Administrative Offices of ALL US COURTS to the Ninth Circuit Ruling by having the DC Circuit Ruling which controls their operations cross-affirm it as well.

This then binds the totality of the US Government itself to the USDC 14-03629/WHA ruling in all forms and Agencies, or Branches. This effectively is the same then as a Publishing Standard without needing the Ninth Circuit to Publish the Ruling.

Transactional Immunity – created permanently by the USDC 14-03629/Ruling and its appeals

The US DC in 14-03629/WHA refused to initiate a Judicially Initiated Prosecution formally denying it twice. For over 15 years the FBI and US Attorneys Offices have refused to initiate any prosecutions in the US6370629 or its related US6393126 Matter. In doing so they have allowed tens of millions of copies of controlled software every year to be sold which contain stolen property. They further refused to prosecute any party for any aspect therein of those actions in the US or beyond. Further, they refused to stop commingling of funds obtained from the sale of that in the US with those moneys obtained from the sales of those stolen IP’s in any of the Nations where US6370629 was filed and then abandoned.

In doing this they created a De-facto Transactional Immunity for any and all parties using the IP in any form or in any device including Computers in private use, commercial uses, and Government uses. Further, they refused to stop the uses of the IP in Weapon Systems as well used in killing tens of millions of civilians over the last 20 years across the middle east and its conflict zones. Or stop those Weapons Vendors from profiting from the sale of those stolen IP’s in their weapons. In doing this they created a formal and provable form of Transactional Immunity for any and all uses. This Immunity itself is like water, it flows across the use model to vaccinate the end-user in all instances as well.

Transactional Immunity WHITEPAPER: in re US6370629

If this is true, and the anonymous immunity in fact vaccinates the uses, and users then all of the Bitcoin impounded by banks for use in everything from Illegal Money Laundering to Terrorism Funding are immune to those seizures and must be formally released to their owners. There are no two ways about it.

> If the Immunity itself which was accorded to Microsoft for the illegal uses of US6370629 in its files system is factual, then the uses of Bitcoin as a terrorism funding source are equally protected.

This is a direct and unintended consequence of the USDC 14-03629/WHA ruling and will persist until a separate settlement is properly reached which addresses those uses and sets a precedent for them with the parties who have suffered those losses, being compensated for the uses of those entities illegally using those IP's. Until that time the Judicial Immunity itself is transactional in form and because of that persists across the uses no matter what the underlying intent was.

See US DOJ AM (Attorney Manual) for the distinctions: https://www.justice.gov/jm/criminal-resource-manual-717-transactional-immunity-distinguished

> Title 18 U.S.C. § 6002 provides use immunity instead of transactional immunity. The difference between transactional and use immunity is that transactional immunity protects the witness from prosecution for the offense or offenses involved, whereas use immunity only protects the witness against the government's use of his or her immunized testimony in a prosecution of the witness -- except in a subsequent prosecution for perjury or giving a false statement.

In the case of the Immunity the US Government granted, as a formal unintended consequence of the USDC 14-03629/WHA ruling the *United States v. Lyons*, 670 F.2d 77, 80 (7th Cir. 1982), *cert. denied*, 457 U.S. 1136. case talks around the issue in detail. The Government formally refused to bring prosecutions against any party using US6370629 IP in any form. The Court in 14-03629/WHA refused to order the USDOJ to institute a Court Ordered JIP (Judicially Initiated Prosecution) and through these two actions created a De-facto issuance of Immunity formally.

Transactional vs Limited or Simple Immunity

Transactional Immunity protects any and all users from any prosecutions. An instance where specific prosecutorial bias was shown further complicated the US Governments position based on the principles of contract law apply in determining the scope of informal immunity. *United States v. Plummer*, 941 F.2d 799, 802 (9th Cir. 1991); *United States v. Britt*, 917 F.2d 353 (8th Cir. 1990), *cert. denied*, 498 U.S. 1090; *United States v. Camp*, 72 F.3d 759 (9th Cir. 1996) [replacing 58 F.3d 491 (9th Cir. 1996)]. The actions of the US Government itself in creating the umbrella of Immunity for the use of these stolen IP's in virtually all software today further complicated the matter with the US v Microsoft settlement as well.

Transactional Immunity WHITEPAPER: in re US6370629

Government failure to formally apply for Immunity from the Court is excused when the Court refuses a JIP

In an instance where the US Government itself violated the standards of formally issuing a letter of Immunity to the Court, doesn't set the construct or effect of the Immunity aside. The Governments requirements for addressing this are only ministerial. *In re Perlin*, 589 F.2d 260 (7th Cir. 1978); *United States v. Frans*, 697 F.2d 188 (7th Cir. 1983), *cert. denied*, 464 U.S. 828 (1983).

When the USDC itself refused to prosecute those parties, it issued a formal immunity to them. One which it continues to use to protect them (and its own illegal uses of Microsoft products illegally containing US637629 methods today). Since Immunized testimony (and all uses pertaining to the US6370629 fraud are) then no Sentencing Judge can possibly interpret or sentence based therein.

See USAM at #725 - https://www.justice.gov/jm/criminal-resource-manual-725-use-immunized-testimony-sentencing-court

> If the witness for whom immunity has been authorized is awaiting sentencing, the prosecutor should ensure that the substance of the witness's compelled testimony is not disclosed to the sentencing judge unless the witness indicates that he or she does not object. This is intended to avoid a claim by the witness that his or her sentence was adversely influenced by the immunized testimony.

The Governments request to block a Court Ordered Judicially Initiated Prosecution constituted the Request for Immunity for all parties.

In the USDC 14-03629/WHA the US Government tacitly asked the Court to block the JIP (Judicially Initiated Prosecution) as asked for repeatedly by Plaintiffs, and this had the same effect of asking for Immunity to be conferred to any and all parties involved in the illegal uses of the US6370629 IP.

While a prosecutors right to refuse Immunity is Unfettered, *US v Bahadar*, 954 F2d 821, 826 (2d Cir 1992), the refusal of the Government to prosecute parties as well as the Courts refusal to initiate a Judicially Initiated Prosecution constitutes an awarding of that Immunity in this case to all of the clients of the Defendants products for those causative actions.

Transactional Immunity WHITEPAPER: in re US6370629

If Testimony doesn't exist and no statement is made – there is nothing to prosecute.

In brown v. walker (1896) the Court held that transactional immunity "operates as a pardon for the offense to which it relates," thus satisfying the constitutional guarantee.

In *New Jersey v. Portash* (1979) the Court held that a defendant's immunized grand jury testimony could not be introduced to impeach his testimony at his trial. Whether the state may introduce immunized testimony to prove perjury has not been decided. In *Portash,* however, the Court conceded, "Testimony given in response to a grant of legislative immunity is the essence of coerced testimony." The essence of the Fifth Amendment's provision is that testimony against oneself cannot be coerced. Any grant of immunity that compels testimony compels one to be a witness against himself—except, of course, that it is "impossible," as the Court said in *Counselman,* for the constitutional guarantee to mean what it says.

In all instances Garrity Use Exemptions are created by the use of the Transactionally Immune Evidence creator softwares.

There is an unexpected consequence of Garrity as well 'The privilege against self-incrimination would be reduced to a hollow mockery if its exercise could be taken as equivalent either to a confession of guilt or a conclusive presumption of perjury. * * * The privilege serves to protect the innocent who otherwise might be ensnared by ambiguous circumstances.' Id., at 557-558, 76 S.Ct. at 641.

The purpose of the 14-03629/WHA Litigation and how it was accomplished

The SOLE PURPOSE of the USDC 14-03629/WHA ruling was to

1. judicially perfect the Section 8 Requirements of the Settlement, Specifically Section §8.7, §8.5, §8.4, §8.3, §8.2, & §8.1 and to document the State and Federal Immunity which had been given to all parties illegally using the IP;

   and

2. to side-step (amend and repeal) the effects of Third Party Enforcement Limitations as defined in Ninth Circuit precedent of DIX v SHASTA COUNTY (1992) and other related Third Party IP Licensing Enforcement standards affirmed.

Both of these core goals were accomplished. As to how, the Matter was filed as a Pre-Enforcement Judicially Perfecting Litigation to test the Settlement Terms. This was necessary because of years of US DOJ and FBI blocking of damage and enforcement rights claim in the matter. This intent is fully defined in the Initial Case Filing, and was obvious from each of the subsequent Motions. Because the Settlements were in fact obtained there a Fraud Related Process, there was a legitimate Pre-Enforcement Controversy which enabled this unique Judicial Move.

In retrospect its something no Lawyer would do professionally because of the permanent ire it would create in the Court against that Attorney's operational standing, and this we believe is the core reason we were forced to take the matter Pro Se. Because the Courts have a longer memory than an Elephant so to speak.

> "Judges never forget any Lawyer making a fool of them, and we certainly did just that. "

USDC 14-03629 and its Unintended Consequences: What did the Ruling Judicially Perfect?

His Honor, Judge Alsup Judicially Perfected each of the key Terms of Section 8 of the Settlements. There were many unintended consequences created by the Ruling of the Court and its appeals which judicially affirmed and perfected the Settlements terms Internationally.

His Honor, Judge Alsup also ruled on the Limitations of the Settlement as in pertaining only to the US Filing of US6370629 and not any of the other Seven instances of the Patent illegally filed and abandoned.

The Unintended Consequences

This had the unintended consequence of judicially perfecting the Plain Text reading of Section §8.7, §8.5, §8.4, §8.3, §8.2, & §8.1 for any and all applications "of any Softwares or other implementations using or relying on the Methods perfected in US6370629 and any of its derivatives using said same Methods or Methods derived from them".

Co-Copyright standing affirmed as well.

It also created a co-copyright standing for any and all purposes protected under the Copyright legal standards and affirmed by the TRIPS treaty and many other documents as well.

Transactional Immunity WHITEPAPER: in re US6370629

The Settlements Terms

In each Motion on the USDC 14-03629/WHA docket, no Motion except those for sanctions were allowed. All motions to overturn the Settlement for Frauds, or Failures in the Terms in each of its Clauses were denied, with full support of each of the Defendants. This proves their willingness to be bound by those terms and conditions globally.,

The Settlement calls for a payment for each patent filing of $300,000 USD which has not been made for any of the seven illegally filed and abandoned instances of US6370629, or any of the 275 derivatives noted in the USPTO Listings. One the USPTO has since intentionally edited to fraudulently cover up its own role in this Government Run Taking (Appropriation) Fraud and international IP Criminal Action.

Apple for instance has 46 (forty six) derivatives at the time of the Ruling which were never paid for, or cross licensed around the legal impact of the seven illegally filed and abandoned instances of US6370629. Microsoft, IBM, HP, Symantec, Sony, the USPS and many others as well, illegally use the Location Based Service components of US6370629 in their Derivatives and are all as such bound by the terms of the Settlement as ruled by the unintended consequences of the USDC actions in 14-03629/WHA.

These same actions impact the Court Operations itself in how PDF Document Headers are processed in US Court and US Government document server systems. The effect of this last statement speaks for itself.

The Settlement is conditional not a complete use release

Because the Settlement itself has a Section §8 which requires post settlement compliance it is Conditional in form. Not a complete release.

Terms to comply with after the Settlement signing

All terms which must be complied with POST SETTLEMENT SIGNING are permanent and will apply as well to any software derived from the methods protected through the terminus of the Patent’s lifetime. The copyrights persist through the full term of the copyright lifetime as do derivatives of those Copyrights against future Software publications derived from them.

US-Only terms and their effect against Non-US Filings.

The Settlement pertains to the US Only Filing, and has no release against any filings of the IP in any other Nations. In all instances those rights fully belong to the Inventor’s therein. Further, the property conversion terms in the original Contract remain in force for those Non-US Filings making them Glassey’s and McNeil's sole property.

Compliance With Section §8 Requirements

Because His Honor, Judge Alsup in USDC 14-03629/WHA did not invalidate Section 8.3 or 8.4 of the Settlement or Section 8.7 and its mandatory requirements, all parties have an obligation to meet the full terms as defined in Section 8 of the Settlement for the use of their software, firmware, and online services derived from or using the Location Based Service and other Methods perfected in US6370629 today.

Section §8.7:Produce Documents showing compliance with Section §8

The requirement of Section §8.7 is that the User will produce any documents necessary to show full compliance with all of Section §8s terms.

Section §8.4:This Requirement is binding on all users and their successors

The requirement of Section §8.4 is that the User will fully comply with all of the terms of Section 8, and especially those in Section §8.1.

Section §8.3: The Successor Clause

Section §8.3 is the Successor Clause defining the end users, and that no party would be licensed to use the Location Based Services perfected in US6370629 or their derivative methods outside of the controls. All parties to the Settlement agreed that this would be the limitation for those controlled by Microsemi[1] is that the User will produce any documents necessary to show full compliance with all of Section §8s terms.

Section §8.2: The Parties Clause

Section §8.2 defined the Parties involved as Digital Delivery Inc, the entity DATUM CORP bought who was the party contracted by Glassey and his company GMT INC of California to file the original US6370629 patent for Glassey, and Glassey and McNeil as members of GMT INC. It fully

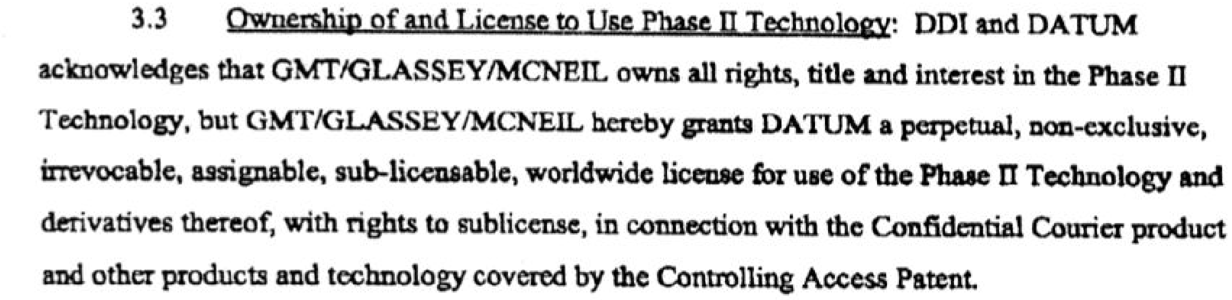
[1] Microsemi Inc is the current Successor to DATUM CORP, and its Digital Delivery Inc entity it subsumed as the original party.

stated that all parties had the legal authority to speak for themselves, and that this agreement would bind their successors as it applied to rights controlled under this agreement.

In no way or form does it convey ownership of Location Based Services (per section 3 of this agreement) to DATUM or its successors but only licenses its use in this specific Patent instance. It also doesn't provide a PARIS ACCORD type release for that Location Based Service uses in any form, nor does any other Clause in the Settlement, “to allow any derivative patents or softwares to be published which use or rely on the Location Based Services which this patent protected”.

Section §3.3 implications as well

Additionally, any which would be filed would be bound by all Section 8 requirements. Finally, there is nothing specific to Section 3.3 to address a release to allow the filing of any other Patents in any form. Under the Paris Accord and subsequent agreements, each Patent filing would need to be fully released and would constitute a separate instance of Patent triggering both the Section 8 requirements and the Payment as defined in the Payment clause as well. See the Section 3,3 text in the next image.



3.3 Ownership of and License to Use Phase II Technology: DDI and DATUM acknowledges that GMT/GLASSEY/MCNEIL owns all rights, title and interest in the Phase II Technology, but GMT/GLASSEY/MCNEIL hereby grants DATUM a perpetual, non-exclusive, irrevocable, assignable, sub-licensable, worldwide license for use of the Phase II Technology and derivatives thereof, with rights to sublicense, in connection with the Confidential Courier product and other products and technology covered by the Controlling Access Patent.

There are further implications in this section, since any Derivative Patent would need to comply with Section §8 compliance and also list Glassey and McNeil as Inventors as well as be Conditionally Assigned because of the Section §8 Compliance Mandates. Imagine what that means to all of the 275 Derivatives of US6370629 which USPTO has been covertly de-listing as Derivatives. This was of course, affirmed by the USDC 14-03629/WHA affirming Section §3.3 of the Settlement and its further implications against Derivatives by both Datum and any other party using this IP as well.

Section §8.1: The California Law Clause and its implications on Derivative Licensing.

Under Section §8.1 parties licensing software or firmware derived from US6370629 must apply the laws of the State of California to those products, services, and online content sessions.

As to how, the USDC 14-03629/WHA Ruling applies California Law to all uses of the US6370629 Methods in the US. Under section 8.1 of the Settlement. As to how this happened, the 14-03629/WHA Court refused to review or invalidate Section §8.1 of the Settlement and found it fully binding. In doing this the Court “Approved Terms require the application of only the laws of the State of California to any and all uses of US6370629”.

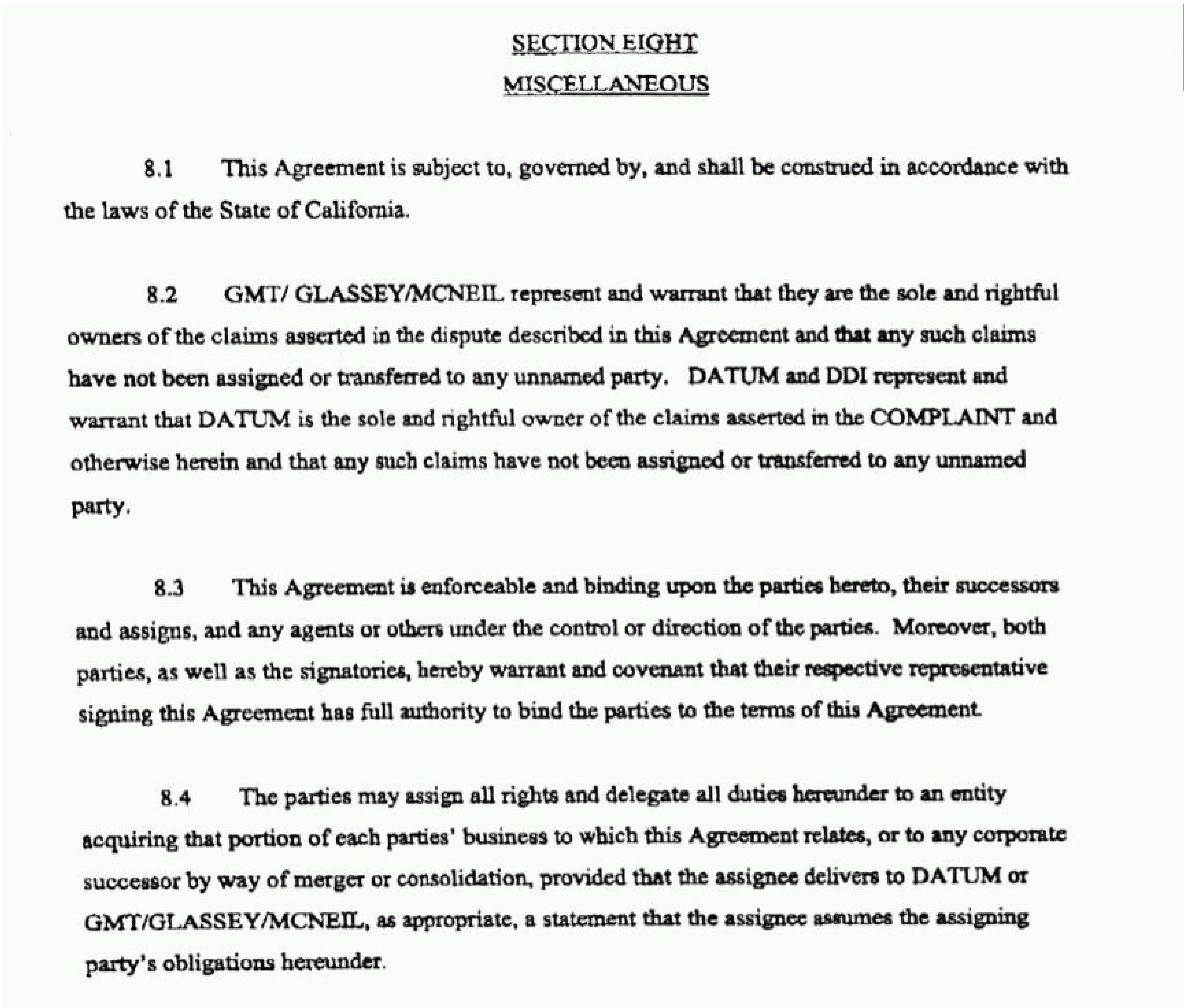
This Clause was installed into the original Settlement because the Settlement does not provide for Commercial Uses. The Settlement only provides for “Development Only” Uses. As such it was never intended that any products derived from it would need commercial licensing or a Choice of Law which could be set at that of the end users Jurisdiction.

Legal Limitations: No Successor may obtain more term standing than the party licensing them has available

One of the key concepts of this DEVELOPMENT ONLY Settlement is that no Successor to the Settlement itself may obtain more term or more standing than that of the party who they obtained that from.

See Sections §8.1 through §8.4 in the next image.

If the previous party you obtained your ability to license from is fully bound by the Laws of the State of California, then any licensing you as their successor would write is then fully bound by that as well. Meaning the Successor to the original Settlement Symmetricom Inc (2003 time frame and Microsemi’s predecessor) was restrained from any licensing outside of the Laws of the State of California for any purposes.



SECTION EIGHT

MISCELLANEOUS

8.1 This Agreement is subject to, governed by, and shall be construed in accordance with the laws of the State of California.

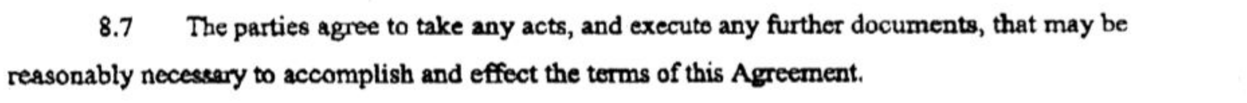
8.2 GMT/ GLASSEY/MCNEIL represent and warrant that they are the sole and rightful owners of the claims asserted in the dispute described in this Agreement and that any such claims have not been assigned or transferred to any unnamed party. DATUM and DDI represent and warrant that DATUM is the sole and rightful owner of the claims asserted in the COMPLAINT and otherwise herein and that any such claims have not been assigned or transferred to any unnamed party.

8.3 This Agreement is enforceable and binding upon the parties hereto, their successors and assigns, and any agents or others under the control or direction of the parties. Moreover, both parties, as well as the signatories, hereby warrant and covenant that their respective representative signing this Agreement has full authority to bind the parties to the terms of this Agreement.

8.4 The parties may assign all rights and delegate all duties hereunder to an entity acquiring that portion of each parties' business to which this Agreement relates, or to any corporate successor by way of merger or consolidation, provided that the assignee delivers to DATUM or GMT/GLASSEY/MCNEIL, as appropriate, a statement that the assignee assumes the assigning party's obligations hereunder.

This is simple legal logic following the ratcheting effect of those terms. Notice, specifically this also applies to their Law Firms meaning it was intended there would be no party immune from these terms including all Lawyers and all Courts, US and State, or International for that matter.

And §8.7

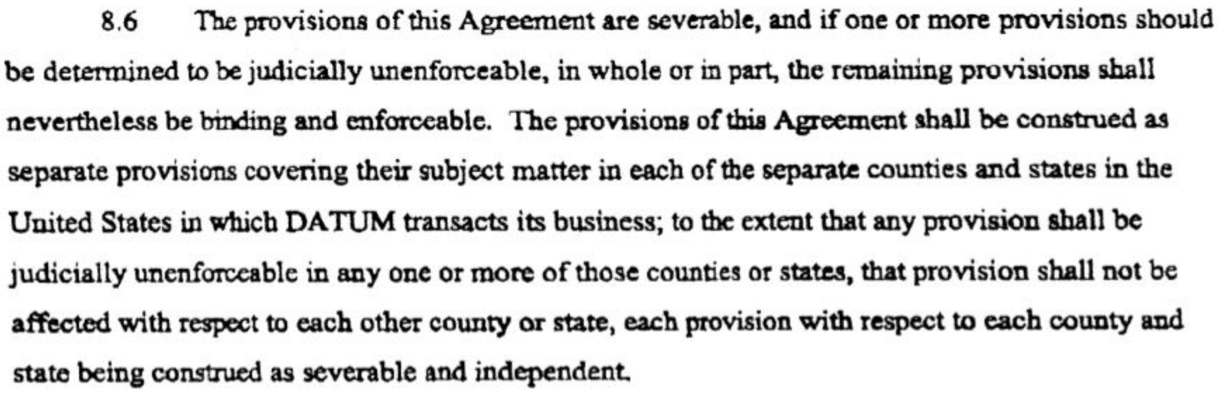


8.7 The parties agree to take any acts, and execute any further documents, that may be reasonably necessary to accomplish and effect the terms of this Agreement.

Section §8.6: The Severability Clause

The Settlement Provisions are Severable per Section §8.6, and any one of them could have been declared unenforceable and void by the Court. But in this matter, the Court and all parties accepted each provision in its plain-text form.

Likewise by refusing to execute provisions of the Severability Claus in the numerous motions Glassey filed, the Court found them all enforceable as did both Appellate Courts who reviewed them. As such they are valid and judicially perfect today.



8.6 The provisions of this Agreement are severable, and if one or more provisions should be determined to be judicially unenforceable, in whole or in part, the remaining provisions shall nevertheless be binding and enforceable. The provisions of this Agreement shall be construed as separate provisions covering their subject matter in each of the separate counties and states in the United States in which DATUM transacts its business; to the extent that any provision shall be judicially unenforceable in any one or more of those counties or states, that provision shall not be affected with respect to each other county or state, each provision with respect to each county and state being construed as severable and independent.

No party to the Litigation filed any objection to meeting those terms or their scope or effect

None of the Defendants filed any papers with the Court to object to those terms and their impacts being enforceable against them in their current and previous instances of those products which became controlled from their inception, by the Ruling of the Court and its unintended consequences. This means they are fully bound by them what ever they are. They accepted them, and had numerous instances where they could have objected or refuted their being bound by those terms and conditions.

In all instances, the entire Military Services Sector, Intelligence Sector, and the Tech Sector watched this trial and was fully aware of who the DOES were in addition to the Named Entities as well.

The parties affected

As to who those named parties are – Named Defendants included Microsoft, Apple, Google, Oracle, Paypal, Ebay, Cisco, Juniper, Microsemi, the IETF itself, and both US Government and California State Government (as proxy for all State Governments). The DOES included Silicon Valley Tech

Sector entities like Facebook, HP, IBM, Symantec, Sony, and many others including those in South Korea and Japan as well.

Finally it included the Weapons Houses including but not limited to General Atomics, Lockheed Martin, BAE, Thales, General Dynamics, as well as a number of other US, British, and EU entities. All Russian and Chinese Entities were excluded from these.

The USDC 14-03629/WHA Ruling excluded the Non-US Instances of the Settlement from the Release Terms of the Settlement making them antitrust issues

The key aspect pertaining to the Non-US Filings was the USDC refusing to consider or otherwise approve their being released by the Language of the US-Only Patent Filing Release. The USDC refused in two separate instances to allow the Court to take Judicial Notice of the seven filings and to review their standing, and as such the plain-text reading of the US Only Release again was perfected eliminating all seven of the Illegally filed instances from the Release effect.

This action codified them as active and open International Antitrust matters ripe for enforcement in Foreign Governments jurisdictions and before the World Court Systems. See Dockets 116 and 118 from the PACER file for USDC 14-03629/WHA for more information on the motions to take notice (and through this include them in any ruling rendered).

The Seven Tigers: All Seven non-US instances of US6370629 were illegally filed and later abandoned

As noted above, US6370629 was illegally filed without authorization and abandoned in seven nations. These are the seven instances of US6370629 which were illegally filed and abandoned.

They are split into two groups, those before the settlement in 1999 and those illegally filed after the settlement in 2000. The 1999 Filings are Australia AP54015/99, Brazil BR9904979A, Canada CA2287596, EU’s EP0997808A3 which fully completed Prosecution and was abandoned by not paying the final publication fee, South Africa ZA9906799. The 2000 post settlement fraudulent filings are Japan JP2000-163379, and South Korea KO2000-0035093.

In all instances none of these are disclosed, or defined in the terms of the Settlement or permitted by the LIMITED USES the Settlement itself has.

The Implications: This makes any uses of their Methods (both as US6370629 instances, and native patents) in any form a Criminal Antitrust Matter in those Jurisdictions.

The refusal of the Court to add those Seven Patents into the Release itself invalidated Microsemi and its predecessors claims that they had global rights from the Settlement, and limited them to just the US Instance. Their failure to contest this in any form supports their understanding of their limitations as well.

Summary: The uses protected by US Securities and Exchange actions

The US Treasury Department’s Securities and Exchange Commission grants Judicial Immunity to any Exchange, Financial System, or Banking enterprise using these US6370629 or derivatives methods in any financial system today. This has broad and sweeping implications which make it literally impossible to prosecute anyone for crimes committed using softwares using or based on those Methods.

US DOJ and US Courts protects any and all uses, including eCurrency uses of US6370629

The US District Courts, and the US Department of Justice grants Judicial Immunity to any party using any Exchange, Financial System, or Banking enterprise using these US6370629 or derivatives methods in any financial system today.

This has even broader and more sweeping implications which make it literally impossible to prosecute anyone for crimes committed using softwares using or based on those Methods. Money Laundering, Drug Trade Transactions, Illegal importation or Wiring of Money to any Nation is legally immune because of these Transactional Immunities granted and fully enforced by the US DOJ and the USDC today.

This effects eCurrency as well.

The Foreign Entities granting the same Judicial Transactional Immunity conveys the same immunity in those nations as well.

S a key concept here, since the seven illegally filed instances of US6370629 are used in those nations for the same uses they are used in the US, the same jurisdictional immunity exists in those nations as well. Its defined in the next two sections in more detail.

Transactional Immunity WHITEPAPER: in re US6370629

1st and 2nd Party Judicially Granted Transactional Immunity

In the US Microsoft and visa vie all Vendors were in 2004 granted transactional immunity from Antitrust Prosecution, and visa vie all Antitrust claims, in the use of software containing stolen IP in the Microsoft Settlement with the US DOJ in the BROWSER SOFTWARE THEFT matter.

This set the standard in the US for Stolen Software IP which was granted immunity from those criminal standings and was fully approved by the US Appellate Court of the DC Circuit. The very Circuit who ruled in (15-01326) this matter that the Settlement terms affirmed by the Ninth Circuits 14-17574 ruling would stand for it and the US Government Agencies it controls as well. The key ones being the US Treasury, and its OFAC or SEC, and the US Department of Justice and Department of Defense as well.

3rd Party Judicially Granted Transactional Immunity

A Third Party using Software which was created and sold using the Transactional Immunity granted the vendors, is equally immune for any and all uses. This is because, like Water, the Transactional Immunity is transcendental in form.

- If you buy software which is protected from Antitrust claims Internationally then simply put you cannot be prosecuted for committing antitrust crimes with it.

- If you buy counterfeit protected software, then you cannot be prosecuted for selling or buying counterfeit wares with it.

- If you buy software which has built in immunity for all white collar criminal uses, then you simply cannot be prosecuted for committing any white collar crime with that software.

Other possible claims may be levied but not those.

US and Global Treaty Impact: How this immunity affects them.

This Transactional Immunity has very broad and detrimental effects on Law Enforcement Treaties and agreements. Some of them reviewed here, but there are of course even wider ones.

AML Money Laundering

Money Laundering – the anonymous ‘washing of assets derived from illegal or unreported sources’ is unprosecutable because of this fraud and the Judicial Immunity granted therein. This is a White Collar Criminal Action and the Transactional Immunity attaches where the act is provable or just an allegation. As such there is no point in charging anyone, nation, or company as they simply cannot be prosecuted. This is also obvious. The Seizure of Privately or Publicly Held Funds is strictly prohibited by International Treaty and constitutes a war crime by the Seizing Government since they are either a direct party to those Judicial Transactional Immunities granted, or a third party who accepted them and as such is bound by their enforcement protections.

Know Your Customer (KYC) is legally required

Know Your Customer requirements for preventing Money Laundering are likewise set aside by the Government's acceptance and protection of the Anonymity standings for Monero and Bitcoin and like trading practices. Only eCurrency Systems or Trading Platforms today have any contractual controls over that as well fully invalidating the seizure of any and all BitCoins for any purpose from Drug, and Weapons Trafficking, to Terrorism Funding as well. The Immunity is NOT selective and without a release from the Settlement Terms of the US6370629 Settlement all parties are tied to its requirements and the standing of the Government Agencies in providing Immunity from those therein.

Source of Funds

Because of the Immunity granted, this cascades into Source of Funds disclosure requirements to prevent Money Laundering, is also moot as well. Like the washing act itself it is protected in the application of anonymous funds, as are also permitted in Monero and BitCoin trading practices fully.

As such there is no requirement to meet any demand to disclose Source of Funds to any legal representative who does not hold immunity from those matters. This means US, EU, UK and their related law enforcement parties have no legal authority to demand source of funds information.

Beneficial Ownership Requirements

Because of the Immunity granted, this cascades into Beneficial Ownership disclosure requirements to prevent Money Laundering, is also moot as well. Like the washing act itself it is protected in the application of anonymous funds, as are also permitted in Monero and BitCoin trading practices fully.

As such there is no requirement to meet any demand to disclose Beneficial Ownership to any legal representative who does not hold immunity from those matters. This means US, EU, UK and their related law enforcement parties have no legal authority to demand source of funds information.

Rule of Law implications Globally

The Rule of Law implications are very very serious. They provide a basis for stopping everything from Financial Seizures to demanding those made since the ruling in 2014 be returned and interest paid against those fund as well.

Invalidating tens of thousands of Convictions Globally over the last decade or so

In the UK and US for instance there are many implications including invalidating virtually all white collar criminal prosecutions which used or relied on software with the stolen IP inside it. This includes aircraft navigation systems and their use in smuggling as well as monetary transactions in all aspects. It pertains to frauds in the Securities Framework as well, and invalidates the Madoff and other Convictions simply because of the transactions themselves. It would not invalidate even invalidate Conspiracy matters using any digital transport tied to the use of the Stolen IP as well.

Transactional Immunity WHITEPAPER: in re US6370629

Section 2 – For Technologists

This document applies to all eCurrency Systems using US6370629

The scope of this document applies and is focused on eCurrencies, but clearly applies to all uses of US6370629 in Weapons, Commercial Softwares, Banking Systems and much more.

The first step is to tell you want US6370629 is and what it provides methods for. US6370629 provides methods for creating and using Cryptographic Tokens representing time and location and other Data, in this case eCurrency information. It allows for the use of these as Data Blobs which are processed by other Programs and in instances, they can be used to trigger those events inside programs as well – as well as creating software interrupts. It originated in work being done inside the American Bar Association’s Information Security Committee in the mid to late 1990s on “creating digital evidence which would meet the legal requirements for National level reporting models” and quickly morphed from there into Weapons and Banking Systems. Today there are not many systems who don't use it in one or many areas of their functionality.

Conceptually, US6370629 creates a method of using Time and or Time/Location or just Location information as control practices. It was designed originally as an inertial navigation and document control practice as part of a larger effort being worked on to turn a National Clock into a Policy Control Element instead of just something which tics away. US6370629 has become one of the most significant patents in the world, controlling aspects of virtually all computing today.

The eCurrencies and their Methods

Today, eCurrencies are the rage in providing peer to peer financial services. In all instances they are systems representing value in a secure crypto-tokenized manner. They all depend on US6370629 in one or more areas and cannot work without it.

BitCoin for instance relies on the US6370629 and Merkel Hash patents (from Haber/Stronetta) for all of their core crypto functions. The DLT, Distributed Ledger Technology, itself is based on Haber and Stronetta work at Bell Labs the the underlying tokenization and timestamp controlled token model, from Glassey's work in creating Location Based Services. In all instances, BitCoin cannot function without both of these patented areas of technology. The US6370629 Patent is still in effect and will be until 2022 so it is of core importance here since there are post-settlement use requirements for using it.

Transactional Immunity WHITEPAPER: in re US6370629

Cryptographic Mining Services

In understanding Mining of eCurrencies lets focus on BitCoin itself. In Bitcoin a there are generally speaking, two types of Nodes. Mining and Processing Nodes. A node is a computer that runs the Bitcoin mining software and serves as an element in the distributed processing framework of all BitCoin Mining Services.

Each node will send information to a few other nodes that it “knows” as part of its Web of Known Nodes, who also each will relay the information to nodes that they know, etc. That way based on a thing called Inter-Nodal Latency the Work of Mining is published Globally in a reasonably fast manner.

Mining Nodes group outstanding transactions into blocks and add them to the blockchain. This is done in the Mining Nodes by their solving a complex mathematical puzzle that is part of the Bitcoin program, and including the answer they register in the block.

The puzzle that needs solving is to find a number that, when combined with the data in the block and passed through a hash function, produces a result that is within a certain range. This is much harder than it sounds. This number is called a "nonce". A NONCE is a cryptographic term meaning “a concatenation of a ‘number used once.’". In the BitCoin algorithm a NONCE is an integer between 0 and 4,294,967,296.)

The process of finding this number is based on guessing at random. Each guess represents a swing of the pick ax at the ore in the Mine.

The hash function makes it nearly impossible to predict what the output will be. The miners computationally “swing their pick axe” and guess the mystery number and apply the hash function to the combination of that guessed number and the data in the block.

To be possibly within the realm of correctness to have value, the resulting hash has to start with a pre-established number of zeros.

There's no way of knowing which number will work, because two consecutive integers will give wildly varying results. What's more, there may be several nonces that produce the desired result, or there may be none. In all instances the Miners just start another “Swing” of their computational pick axes when they fail either in the same or a difference block configuration.

The first miner to get a resulting hash within the desired range posts a message to its computational-success to the rest of the network. When that message is received it creates a Process Interrupt which tells all the other miners immediately stop work on that block and to load a new block configuration and then to start trying to figure out the mystery number for the next one.

As a reward for its work, the miner with the correct answer gets some new Bitcoin. This amount varies but at the time of writing, the reward is 12.5 Bitcoins meaning 12.5 times the current price per Bitcoins.

The things that constrain the value earned are both the luck of the miners and the sheer number of miners involved in attempting to fit a number into this correctness curve that works. Each Calculation takes a fixed amount of time and so the more miners you have ganged together, the more likely (from a statistical standpoint you are to find a correct answer. One the effort is completed the Miner is credited with what is referred to as a 'block reward' plus transaction fees.

Also, the number of Bitcoins awarded as a reward for solving the puzzle will decrease. It's 12.5 now, but it halves every four years or so (the next halving is expected in 2020-21). Finally unless the value of Bitcoin relative to cost of electricity and hardware goes up over the next few years to partially compensate this reduction, its value is even more impacted.

Additionally there are other hurdles to address and US6370629

The difficulty of the calculation (the required number of zeros at the beginning of the hash string) is adjusted frequently, so that with a specific set of hardware benchmark systems, it takes on average about 10 minutes to process a block.

That is the amount of time coded into the BitCoin algorithm to theoretically create a steady and diminishing flow of new coins until the maximum number of 21 million is reached. This is expected in 2140 meaning that with the last 4M coins to be mined (there are about 17M of them mined already) they will take that amount of time making the actual flow of newly found coins rather small relative to the amount of computational overhead they require.

Once the token is proven mathematically correct, it is then timestamped and turned into a US6370629 controlled data instance for inclusion into the BlockChain structure.

But that is Bitcoin in a nutshell.. Now we get to the concept of Consensus Algorithms.

Consensus Algorithms and US6370629

Any time an eCoin is certified through a consensus process a certified timestamp is created. That timestamp may contain any number of key points included who and how it was created, and how long its digital certificate remains valid if one is used. In all instances those efforts step directly into the areas US6370629 controls, so in addition to Block Chain management which is controlled by both US6370629 and the Haber/Stronetta Merkel Hash storage service patent, there are other uses of US6370629 in each consensus process.

Transactional Immunity WHITEPAPER: in re US6370629

Several difference Consensus Methods exist in eCurrencies, some based on the concept of Mining, others based on simple computer generated digital cryptographic tokens, but in all instances, the Tokens and their Conveyance are controlled by US6370629 Methods in all instances.

For the purpose of outlining those issues, we go into some technical detail about the processes, and provide hyperlinks to online documents fully describing the ICO Processes in each of the three key eCurrencies we take into this brief.

All of the non-governmental issued eCoins need a Consensus Algorithm to properly identify it. Government issued coins use direct token authentication as their proof of standing.

DLT: Block Chaining for Distributed Ledger Functionality

Block Chaining has been lauded as the answer to everything, and while it helps in pBFT (practical Byzantine Fault Tolerance) in peer to peer networks, it has limits. It also has a tremendous reliance on both Haber Stronetta works (there are at least four patents), and the Glassey/McNeil work in US6370629.

Block Chaining is based on a Merkel Hash based variant of the Surety and Bell Labs patents both worked on. The uses of the tokens in the Wallet, and in the exchange once extracted from the Ledger is all US6370629.

Bitcoin and its POW Consensus Algorithm

Overall, the most important the engine that drives consensus in Bitcoin is the Proof of Work consensus protocol. Systems configured only as Miners use a specific full node to compete in mining blocks in order to earn the block reward that is issued for each successfully mined and validated block. Nakamoto Consensus can be broken down into roughly 4 parts.

- Proof of Work (PoW)
- Block Selection
- Scarcity
- Incentive Structure

There is an inherent cost for running these repeated mining attempts. The cost of this mining process is electricity, which has a real world financial value. It is this real-world cost of electricity and the capital acquisition costs of the Miners which creates each issued BTC for each block mined, an real-world value. Then in the case of Bitcoin that is further abstracted by a market value statement created in the exchanges which trade and covert Bitcoin to fiat (real world money).

PoW in Bitcoin is designed to prevent what is called double spending. While the digital signature scheme within the UTXO model (based on US6370629 methods) provides the verifiable ownership of transaction outputs to be spent, it does not enable prevention of double spending. The blockchain based on the Haber/Stronetta adaptations is a chain of US6370629 timestamped data blocks containing transactions with each block hashed (cryptographically tied through the Merkel Hash process) to connect it to the previous one.

This provides immutability to the blockchain, but how can you tell if the chain that you are on is the correct chain? This is where PoW comes in.

Contributing to mining is based on computational power, the more power within the network that you have, the more likely you are to mine a block.

The process however is stochastic, and as such it is functionally a lottery with random chance of who will win. Because of this is is mechanically impossible to know who will win the next round and the cost to participate will always continue to increase.

Because of this model, the longest chain submitted or maintained is considered the most valid chain because it came from the largest pool of computational power. The validation rules ensure that proposed blocks have the requisite computational work performed in order to be accepted.

Further, there is a reliance on honesty in the nodes, such that as long as the longest chain and majority of the network's hashing power is controlled by honest nodes. As such the honest chains will grow the fastest and outpace competing chains.

The result of this system is that once the cryptographic puzzle for the mining round is solved, a miner proposes the US6370629 based block to the network, the network of Member Nodes "validates the block if all the transactions within the block are not double spent" and then if properly certified the block is added to the longest chain.

The block selection process utilized by Nakamoto Consensus differentiates it from other consensus models. The model is predicated on a PoW design which refers to the "lottery" process for miners competing to "win the block reward for mining the proposed next block".

Consensus Algorithm: POS

In the POS consensus algorithm, instead of creating a Mining Array and operating it to produce the hashes in the process to MINE BLOCKS a VALIDATOR Role invests in the coins of the specific eCurrency system. Unlike other POW Systems where parties are paid for their Proof of Work, VALIDATORS in the POS system are paid in transaction fees only.

All Coin instances in a POS system exist from the first day of the ICO Operations. Meaning there is no future mined coin process.

VALIDATORS are selected for their fiduciary role as a Transaction Validator (and thus they are paid) based on the STAKE (number of eCoin instances) they hold in the system. A VALIDATOR (i.e. a party with eCoins in the System) with 10,000 coins is 10 times more likely to be chosen than someone with 1000 coins as such.

Consensus Algorithm: dPOS

Another methods of POS is to delegate the role of VALIDATORS to specific parties to avoid super critical aggregations where parties with massive numbers of coins wind up as validators and then can manipulate the validator availability scheme. In both instances (POS vs dPOS) the process has its own limitations.

Posting BTC (the Wallet)

An eCoin Wallet is a duel File Content Management Application for a number of eCOIN API's (Application programming Interfaces). They use the Coin Service Routines to access the Wallet Content, Update it, and perform various bookkeeping and fiduciary routines.

The eCurrency Wallet Functions (Create Coin Instance, Spend Coin, Recover Coin, Delete Coin) all rely on US6370629 digital timestamps with location information inside them. For each COIN posted to a Wallet Entity

The Legal Implications

Bitcoin and Monero Anonymity Constructs invalidate all KYC requirements

Any system dependent in any manner for its use of US6370629 has judicially transactional immunity poured atop it like honey. It flows into every part of the system and its immunity vaccinates any party from prosecution for any act with that system.

The Governments allow trading of Bitcoin and Monero tokens with anonymity. That means those tokens are immune from Know Your Customer requirements as ludicrous as it sounds.

If this is true, and the anonymous immunity in fact vaccinates the uses, and users then all of the Bitcoin impounded by banks for use in everything from Illegal Money Laundering to Terrorism

Funding are immune to those seizures and must be formally released to their owners. There are no two ways about it. If the Immunity itself which was accorded to Microsoft for the illegal uses of US6370629 in its files system is factual, then the uses of Bitcoin as a terrorism funding source are equally protected. This is a direct and unintended consequence of the USDC 14-03629/WHA ruling and will persist until a separate settlement is properly reached which addresses those uses and sets a precedent for them with the parties who have suffered those losses, being compensated for the uses of those entities illegally using those IP’s. Until that time the Judicial Immunity itself is transactional in form and because of that persists across the uses no matter what the underlying intent was. See US DOJ AM (Attorney Manual) for the distinctions: https://www.justice.gov/jm/criminal-resource-manual-717-transactional-immunity-distinguished

Title 18 U.S.C. § 6002 provides use immunity instead of transactional immunity. The difference between transactional and use immunity is that transactional immunity protects the witness from prosecution for the offense or offenses involved, whereas use immunity only protects the witness against the government's use of his or her immunized testimony in a prosecution of the witness -- except in a subsequent prosecution for perjury or giving a false statement.

In the cased of the Immunity the US Government granted, as a formal unintended consequence of the USDC 14-03629/WHA ruling the *United States v. Lyons*, 670 F.2d 77, 80 (7th Cir. 1982), *cert. denied*, 457 U.S. 1136. case talks around the issue in detail. The Government formally refused to bring prosecutions against any party using US6370629 IP in any form. The Court in 14-03629/WHA refused to order the USDOJ to institute a Court Ordered JIP (Judicially Initiated Prosecution) and through these two actions created a De-facto issuance of Immunity formally.

Transactional Immunity protects any and all users from any prosecutions. An instance where specific prosecutorial bias was shown further complicated the US Governments position based on the principles of contract law apply in determining the scope of informal immunity. *United States v. Plummer*, 941 F.2d 799, 802 (9th Cir. 1991); *United States v. Britt*, 917 F.2d 353 (8th Cir. 1990), *cert. denied*, 498 U.S. 1090; *United States v. Camp*, 72 F.3d 759 (9th Cir. 1996) [replacing 58 F.3d 491 (9th Cir. 1996)]. The actions of the US Government itself in creating the umbrella of Immunity for the use of these stolen IP’s in virtually all software today further complicated the matter with the US v Microsoft settlement as well.

In an instance where the US Government itself violated the standards of formally issuing a letter of Immunity to the Court, doesn't set the construct or effect of the Immunity aside. The Governments requirements for addressing this are only ministerial. *In re Perlin*, 589 F.2d 260 (7th Cir. 1978); *United States v. Frans*, 697 F.2d 188 (7th Cir. 1983), *cert. denied*, 464 U.S. 828 (1983).

Since Immunized testimony (and all uses pertaining to the US6370629 fraud are) then no Sentencing Judge can possibly interpret or sentence based therein. See USAM at #725 -

https://www.justice.gov/jm/criminal-resource-manual-725-use-immunized-testimony-sentencing-court

If the witness for whom immunity has been authorized is awaiting sentencing, the prosecutor should ensure that the substance of the witness's compelled testimony is not disclosed to the sentencing judge unless the witness indicates that he or she does not object. This is intended to avoid a claim by the witness that his or her sentence was adversely influenced by the immunized testimony.