బిట్‌కాయిన్: ఒక మనిషికి–మనిషికి మధ్య ఎలక్ట్రానిక్ నగదు వ్యవస్థ

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Translated in Telugu from bitcoin.org/bitcoin.pdf by Charaen

సారాంశం. ఒక సహకార ఆధారిత డిజిటల్ నగదు పద్ధతి ద్వారా, ప్రజలు తమ డబ్బును నేరుగా ఒకరి నుండి మరొకరికి ఆన్‌లైన్‌లో పంపుకోవచ్చు, బ్యాంకులు లేదా ఇతర ఆర్థిక సంస్థల అవసరం లేకుండా. డిజిటల్ సంతకాలు ఈ ప్రక్రియలో కొంత భద్రతను అందిస్తాయి. అయితే, ఒకరు ఒకే డబ్బును రెండుసార్లు ఖర్చుచేసే మోసాన్ని (డబుల్-స్పెండింగ్) నివారించేందుకు మూడవ పార్టీ నమ్మకం ఇంకా అవసరం అనే సమస్య ఉంది. మేము ఈ సమస్యకు ఒక పరిష్కారం సూచిస్తున్నాము: ఒక సహకార నెట్‌వర్క్ ద్వారా అందరూ కలిసి పని చేయడం. ఈ నెట్‌వర్క్ ప్రతి లావాదేవీని ఒక చైన్‌లో జోడిస్తుంది, దానిని మార్చడానికి ముందు చేసిన పనిని మళ్ళీ చేయాలి. ఈ పద్ధతిలో, అతి పెద్ద చైన్ అనేది నిజంగా జరిగిన విషయాల క్రమం మరియు అత్యధిక కంప్యూటర్ శక్తి నుండి వచ్చినదనే రుజువుగా ఉపయోగపడుతుంది. నెట్‌వర్క్ మీద దాడి చేయాలనుకునేవారు కన్నా ఎక్కువ కంప్యూటర్ శక్తి ఉన్న వారు ఈ చైన్‌ను నిర్మాణం చేస్తారు.ఈ నెట్‌వర్క్ చాలా సాధారణమైనది. ప్రజలు తమ సందేశాలను పంపుకుంటూ, ఎప్పుడైనా నెట్‌వర్క్‌ను విడిచి మళ్ళీ చేరుకోవచ్చు. వారు వెళ్ళిపోయిన సమయంలో ఏమి జరిగిందో తెలుసుకోవడానికి అతి పెద్ద ప్రూఫ్-ఆఫ్-వర్క్ చైన్‌ను వారు అంగీకరిస్తారు.

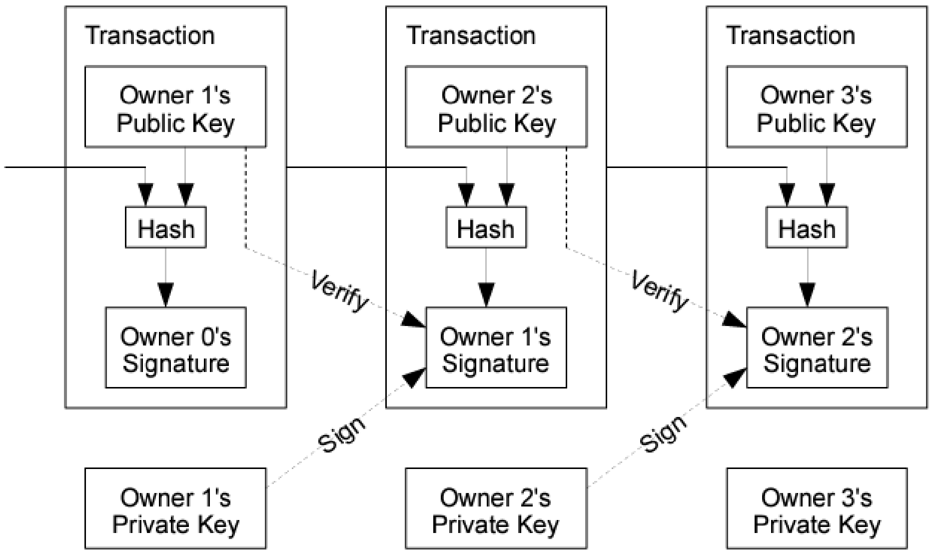
1. పరిచయం

ఇంటర్నెట్ పై వాణిజ్యం దాదాపు మొత్తంగా విశ్వసనీయమైన మూడవ పార్టీలుగా పనిచేసే ఆర్థిక సంస్థలపై ఆధారపడి ఎలక్ట్రానిక్ చెల్లింపులను ప్రాసెస్ చేయడంలో ఉంది. ఈ వ్యవస్థ ఎక్కువ భాగం లావాదేవీలకు సరిపోతుంది, కానీ ఇది విశ్వాసాధారిత మోడల్‌లోని స్వాభావిక బలహీనతల నుండి ఇంకా బాధపడుతుంది. పూర్తిగా అనులోమ కాని లావాదేవీలు నిజానికి సాధ్యపడవు, ఎందుకంటే ఆర్థిక సంస్థలు వివాదాలను మధ్యవర్తిత్వం చేయకుండా ఉండలేవు. మధ్యవర్తిత్వం ఖర్చు లావాదేవీ ఖర్చులను పెంచుతుంది, కనిష్ఠ వ్యవహారిక లావాదేవీ పరిమాణాన్ని పరిమితం చేస్తుంది, చిన్న అనధికారిక లావాదేవీల సాధ్యతను తొలగిస్తుంది, మరియు అనులోమ కాని సేవలకు అనులోమ కాని చెల్లింపులను చేయలేని విషయంలో విస్తృత ఖర్చు ఉంది. విపరీత సాధ్యతతో, విశ్వాసం అవసరం వ్యాపిస్తుంది. వర్తకులు తమ గ్రాహకుల పట్ల జాగ్రత్తగా ఉండాలి, అవసరం లేని సమాచారం కోసం వారిని ఇబ్బంది పెడుతుంది. ఒక నిశ్చిత శాతం మోసాన్ని తప్పనిసరిగా ఉంటుంది. ఈ ఖర్చులు మరియు చెల్లింపు అనిశ్చితులను భౌతిక నాణెం ఉపయోగించి వ్యక్తిగతంగా తప్పించుకోవచ్చు, కానీ విశ్వసనీయమైన పార్టీ లేకుండా సమాచార చానల్ ద్వారా చెల్లింపులు చేయడానికి ఏ యంత్రాంగం లేదు. అవసరం అయినది విశ్వాసం బదులుగా క్రిప్టోగ్రాఫిక్ ప్రూఫ్ ఆధారిత ఎలక్ట్రానిక్ చెల్లింపు వ్యవస్థ, దీని ద్వారా ఏ

రెండు అంగీకారపూర్వక పార్టీలు కూడా విశ్వసనీయమైన మూడవ పార్టీ అవసరం లేకుండా పరస్పరం నేరుగా లావాదేవీ చేయగలరు. కంప్యూటేషనల్ ప్రాక్టికల్ గా రివర్స్ చేయలేని లావాదేవీలు అమ్మకదారులను మోసం నుండి రక్షిస్తాయి, మరియు కొనుగోలుదారులను రక్షించేందుకు రొటీన్ ఎస్క్రో యంత్రాంగాలను సులభంగా అమలు చేయవచ్చు. ఈ పేపర్‌లో, మేము సహకార నెట్‌వర్క్ ఉపయోగించి ఒక పీర్-టు-పీర్ పంచాంగ సమయ సేవర్‌ను ఉపయోగించి డబుల్-స్పెండింగ్ సమస్యకు ఒక పరిష్కారాన్ని ప్రతిపాదిస్తున్నాము, ఇది లావాదేవీల క్రమాన్ని కంప్యూటేషనల్ ప్రూఫ్ ఆఫ్ ది క్రానాలాజికల్ ఆర్డర్ ఉత్పత్తి చేయడం. సిస్టమ్ సురక్షితంగా ఉంటుంది అంత కాలం నిజాయితీపరులైన నోడ్‌లు ఏదైనా సహకరించే దాడిదారుల గ్రూప్ కంటే ఎక్కువ CPU శక్తిని కలిగి ఉంటే.

2. లావాదేవీలు

మేము ఒక ఎలక్ట్రానిక్ నాణెంను డిజిటల్ సంతకాల శృంఖలగా నిర్వచిస్తున్నాము. ప్రతి యజమాని గత లావాదేవి మరియు తదుపరి యజమాని యొక్క పబ్లిక్ కీ యొక్క హాష్‌ను డిజిటల్లీ సంతకించి, ఈ రెండింటిని నాణెం చివరికి జోడిస్తూ నాణెంను తర్వాతి యజమానికి బదిలీ చేస్తారు. గ్రహీత సంతకాలను తనిఖీ చేసి యజమానుల శృంఖలను నిర్ధారించవచ్చు.

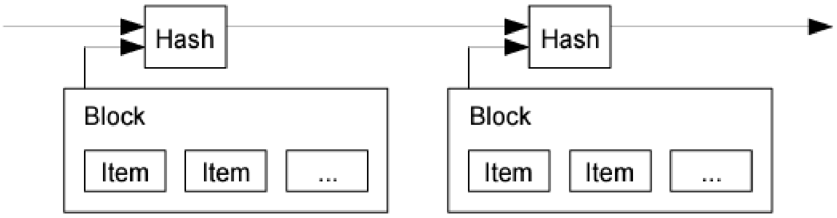


సమస్య ఏమిటంటే గ్రహీత నాణెం యజమానులలో ఒకరు డబుల్-స్పెండ్ చేయలేదని తనిఖీ చేయలేరు. సాధారణ పరిష్కారం ప్రతి లావాదేవిని డబుల్ స్పెండింగ్ కోసం తనిఖీ చేసే విశ్వసనీయ కేంద్రీయ అధికారిని, లేదా టాంకశాల పరిచయం చేయడం. ప్రతి లావాదేవీ అనంతరం, నాణెంను కొత్త నాణెం జారీ చేయడానికి మింట్‌కు తిరిగి పంపాలి, మరియు నేరుగా మింట్ నుండి జారీ చేయబడిన నాణేలు మాత్రమే డబుల్-స్పెండ్ చేయబడలేదని నమ్మబడతాయి.ఈ

పరిష్కారంతో సమస్య ఏమిటంటే, మొత్తం డబ్బు వ్యవస్థ యొక్క భవిష్యత్తు మింట్‌ను నడిపే సంస్థ మీద ఆధారపడుతుంది, ప్రతి లావాదేవీ వారి ద్వారా జరగాలి, బ్యాంకు వలె. గత యజమానులు ఏ ముందు లావాదేవీలను సంతకించలేదని గ్రహీతకు తెలియాలంటే మనకు ఒక మార్గం అవసరం. మన ఉద్దేశ్యాల కోసం, మొదటి లావాదేవీనే లెక్కిస్తాము, కాబట్టి మేము తర్వాత డబుల్-స్పెండ్ యత్నాల గురించి పట్టించుకోము. లావాదేవీ లేనిదానిని నిర్ధారించడానికి ఏకైక మార్గం అన్ని లావాదేవీల గురించి తెలుసుకోవడం. మింట్ ఆధారిత మోడల్‌లో, మింట్ అన్ని లావాదేవీలను తెలుసుకుని, ఏది ముందు వచ్చిందో నిర్ణయించింది. విశ్వసనీయ పార్టీ లేకుండా దీన్ని సాధించడానికి, లావాదేవీలను బహిరంగంగా ప్రకటించాలి, మరియు వాటిని అందుకున్న క్రమంలో ఒకే చరిత్రను అంగీకరించే వ్యవస్థ అవసరం. ప్రతి లావాదేవీ సమయంలో నోడ్‌ల మెజారిటీ అది మొదట అందుకున్నదని ఒప్పుకున్నారని గ్రహీతకు రుజువు అవసరం.

3. టైమ్‌స్టాంప్ సర్వర్

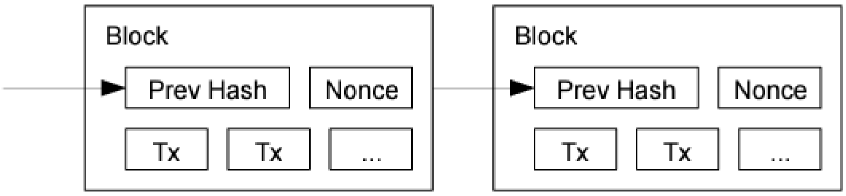
మేము సూచించే పరిష్కారం ఒక టైమ్‌స్టాంప్ సర్వర్‌తో ప్రారంభమవుతుంది. ఒక టైమ్‌స్టాంప్ సర్వర్ టైమ్‌స్టాంప్ చేయబడాల్సిన ఐటెమ్‌ల బ్లాక్‌ను తీసుకొని, దాని హాష్‌ను విస్తృతంగా ప్రచురిస్తుంది, ఉదాహరణకు ఒక వార్తాపత్రికలో లేదా యూజ్‌నెట్ పోస్ట్‌లో [2-5]. టైమ్‌స్టాంప్ డేటా ఆ సమయంలో ఉండాల్సినది అని రుజువు చేస్తుంది, స్పష్టంగా, హాష్‌లో చేరడానికి. ప్రతి టైమ్‌స్టాంప్ దాని హాష్‌లో మునుపటి టైమ్‌స్టాంప్‌ను చేర్చుకుంటూ, ఒక చైన్‌ను ఏర్పరచి, ప్రతి అదనపు టైమ్‌స్టాంప్ దాని ముందువాటిని బలపరచుతుంది.



4. ప్రూఫ్-ఆఫ్-వర్క్

సహకార ఆధారిత విధానంలో ఒక వితరణ టైమ్‌స్టాంప్ సర్వర్‌ను అమలు చేయడానికి, మేము వార్తాపత్రికల లేదా యూజ్‌నెట్ పోస్ట్‌ల కంటే ఆడమ్ బ్యాక్‌ను హాష్‌కాష్ [6] లాంటి ప్రూఫ్-ఆఫ్-వర్క్ వ్యవస్థను ఉపయోగించాలి. ప్రూఫ్-ఆఫ్-వర్క్ ప్రక్రియ ఒక విలువను స్కాన్ చేసి, దాన్ని SHA-256 వంటి పద్ధతిలో హాష్ చేసినప్పుడు, ఆ హాష్ సున్నా బిట్లతో ప్రారంభమవుతుంది. అవసరమైన సున్నా బిట్ల సంఖ్యలో సగటు పని గణనీయంగా వృద్ధి చెందుతుంది మరియు ఒకే ఒక్క హాష్ అమలు చేసి దీన్ని ధృవీకరించవచ్చు.

మా టైమ్‌స్టాంప్ నెట్‌వర్క్ కోసం, మేము బ్లాక్‌లో ఒక నాన్స్‌ను పెంచుతూ ప్రూఫ్-ఆఫ్-వర్క్‌ను అమలు చేస్తాము, దాని వలన బ్లాక్‌కు అవసరమైన సున్నా బిట్లతో హాష్ వచ్చే విలువ కనుగొనబడుతుంది. ప్రూఫ్-ఆఫ్-వర్క్‌ను సంతృప్తి పరచడానికి అవసరమైన CPU శ్రమ వ్యయపరచబడిన తర్వాత, పనిని తిరిగి చేయకుండా బ్లాక్‌ను మార్చలేము. దాని తర్వాత చైన్ చేయబడిన తరువాతి బ్లాక్‌లు ఉండగా, బ్లాక్‌ను మార్చాలంటే తర్వాతి అన్ని బ్లాక్‌ల పనిని తిరిగి చేయాలి.



ప్రూఫ్-ఆఫ్-వర్క్ మెజారిటీ నిర్ణయ నిర్ధారణలో ప్రాతినిధ్యం సమస్యను కూడా పరిష్కరిస్తుంది. మెజారిటీ ఒక-IP-చిరునామా-ఒక-ఓటు ఆధారంగా ఉంటే, చాలా IPs కేటాయించుకోగల ఎవరైనా దానిని భ్రష్టు పట్టించవచ్చు. ప్రూఫ్-ఆఫ్-వర్క్ అసలు సిద్ధాంతం ఒక-CPU-ఒక-ఓటు గా ఉంటుంది. మెజారిటీ నిర్ణయం అత్యధిక ప్రూఫ్-ఆఫ్-వర్క్ ప్రయత్నం పెట్టబడిన అతి పొడవైన చైన్ ద్వారా ప్రాతినిధ్యం చేయబడుతుంది. ఒక మెజారిటీ సీపీయూ శక్తి నిజాయితీపరులైన నోడ్లు నియంత్రిస్తే, నిజాయితీపరులైన చైన్ అతి వేగంగా పెరుగుతుంది మరియు ఏదైనా పోటీ చైన్‌లను మించిపోతుంది. గతంలో ఉన్న బ్లాక్‌ను మార్చాలనుకునే దాడిదారుడు ఆ బ్లాక్ మరియు దాని తర్వాత ఉన్న అన్ని బ్లాక్‌ల ప్రూఫ్-ఆఫ్-వర్క్‌ను తిరిగి చేయాలి మరియు తర్వాత నిజాయితీపరులైన నోడ్ల పనిని అందుకుని దాటాలి. తర్వాత బ్లాక్‌లు జోడించబడినట్లుగా నెమ్మదిగా ఉన్న దాడిదారుడు అందుకునే అవకాశం క్రమంగా తగ్గుతుందని మేము తర్వాత చూపిస్తాము. హార్డ్‌వేర్ వేగం పెరుగుదల మరియు సమయం పాటు నోడ్లను నడపడానికి ఆసక్తి వ్యత్యాసం పరిహారంగా, ప్రూఫ్-ఆఫ్-వర్క్ కష్టతను గంటకు సగటు సంఖ్యలో బ్లాక్‌ల లక్ష్యంతో చలించే సగటు ఆధారంగా నిర్ధారిస్తారు. అవి చాలా వేగంగా ఉత్పత్తి అయితే, కష్టత పెరుగుతుంది.

5. నెట్‌వర్క్

నెట్‌వర్క్‌ను నడపడానికి దశలు ఈ క్రింది విధంగా ఉంటాయి:

1) కొత్త లావాదేవీలు అన్ని నోడ్‌లకు ప్రసారం చేయబడతాయి.

2) ప్రతి నోడ్ కొత్త లావాదేవీలను ఒక బ్లాక్‌లో సేకరిస్తుంది.

3) ప్రతి నోడ్ దాని బ్లాక్‌కు ఒక కఠినమైన ప్రూఫ్-ఆఫ్-వర్క్‌ను కనుగొనేందుకు పని చేస్తుంది.

4) ఒక నోడ్ ప్రూఫ్-ఆఫ్-వర్క్‌ను కనుగొనినప్పుడు, దాని బ్లాక్‌ను అన్ని నోడ్‌లకు ప్రసారం చేస్తుంది.

5) నోడ్‌లు దానిలోని అన్ని లావాదేవీలు చెల్లుబాటు అయ్యేవి మరియు ఇప్పటికే ఖర్చు చేయబడలేదని తెలుసుకున్నప్పుడే బ్లాక్‌ను ఆమోదిస్తాయి.

6) నోడ్‌లు చైన్‌లో తర్వాతి బ్లాక్‌ను సృష్టించే పనిలో తమ ఆమోదాన్ని వ్యక్తం చేస్తాయి, ఆమోదించబడిన బ్లాక్ యొక్క హాష్‌ను మునుపటి హాష్‌గా ఉపయోగిస్తూ.

నోడ్‌లు ఎల్లప్పుడూ అతి పొడవైన చైన్‌ను సరైనదిగా పరిగణించి, దాన్ని విస్తరించడానికి పని చేస్తాయి. రెండు నోడ్‌లు సమాంతరంగా తర్వాతి బ్లాక్‌ను వేర్వేరు వెర్షన్‌లలో ప్రసారం చేస్తే, కొన్ని నోడ్‌లు ముందుగా ఒకదాన్ని లేదా మరొకదాన్ని అందుకోవచ్చు. ఆ సందర్భంలో, వారు ముందుగా అందుకున్న దానిపై పని చేస్తారు, కానీ మరొక శాఖ అధిక పొడవైనప్పుడు దాన్ని భద్రపరచుకుంటారు. తదుపరి ప్రూఫ్-ఆఫ్-వర్క్ కనుగొనబడి, ఒక శాఖ అధిక పొడవు పొందినప్పుడు ఈ సమానత్వం తెగిపోతుంది; మరొక శాఖపై పని చేస్తున్న నోడ్‌లు అప్పుడు అధిక పొడవు గల శాఖకు మారుతాయి. కొత్త లావాదేవీ ప్రసారాలు తప్పనిసరిగా అన్ని నోడ్‌లను చేరాల్సిన అవసరం లేదు. వాటిని చాలా నోడ్‌లు అందుకుంటే చాలు, త్వరలోనే వాటిని ఒక బ్లాక్‌లో చేర్చబడతాయి. బ్లాక్ ప్రసారాలు కూడా సందేశాలు పడిపోవడం సహించగలవు. ఒక నోడ్ బ్లాక్‌ను అందుకోకపోతే, దాని తర్వాతి బ్లాక్‌ను అందుకుని ఒకటి మిస్ అయ్యానని గ్రహిస్తే దానిని అడుగుతుంది.

6. ప్రోత్సాహకం

సంప్రదాయం ప్రకారం, ఒక బ్లాక్‌లో మొదటి లావాదేవీ ఒక ప్రత్యేక లావాదేవీ అయ్యి ఉంటుంది, ఇది బ్లాక్ సృష్టికర్త యొక్క స్వాధీనంలో కొత్త నాణెం ప్రారంభిస్తుంది. ఇది నెట్‌వర్క్‌ను మద్దతు ఇవ్వడానికి నోడ్‌లకు ఒక ప్రోత్సాహకంగా చేరుస్తుంది, మరియు వాటిని జారీ చేసే కేంద్రీయ అధికారం లేనందున, నాణేలను ప్రారంభ పరిచి సంచలనంలోకి తెచ్చే మార్గంగా ఉంది. నూతన నాణేలను ఒక నిరంతర మొత్తంతో స్థిరంగా జోడించడం

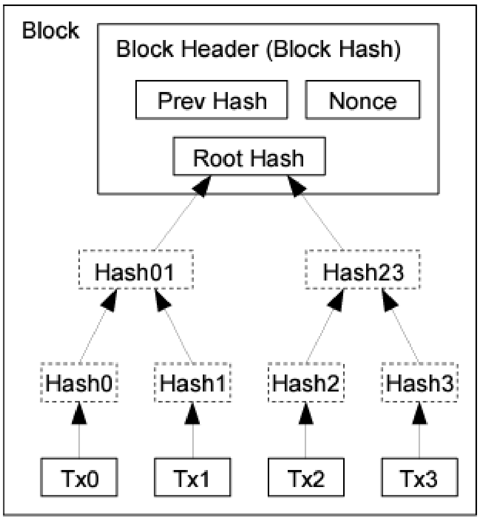
బంగారు గనుల వ్యవసాయిలు వనరులను ఖర్చు చేసి బంగారంను సంచలనంలోకి జోడించడానికి సమానమైనది. మన కేసులో, ఇది CPU సమయం మరియు విద్యుత్ శక్తి ఖర్చు చేయబడుతుంది.

ప్రోత్సాహకం లావాదేవీ రుసుములతో కూడా నిధులించబడవచ్చు. ఒక లావాదేవీ యొక్క ఔట్‌పుట్ విలువ దాని ఇన్‌పుట్ విలువ కంటే తక్కువైతే, తేడా ఒక లావాదేవీ రుసుముగా ఉంటుంది మరియు ఆ లావాదేవీని కలిగి ఉన్న బ్లాక్ యొక్క ప్రోత్సాహక విలువకు జోడించబడుతుంది. నిర్దిష్ట సంఖ్యలో నాణేలు సంచలనంలోకి వచ్చిన తర్వాత, ప్రోత్సాహకం పూర్తిగా లావాదేవీ రుసుములకు మారిపోవచ్చు మరియు పూర్తిగా స్థూలాభివృద్ధి రహితంగా ఉండవచ్చు.

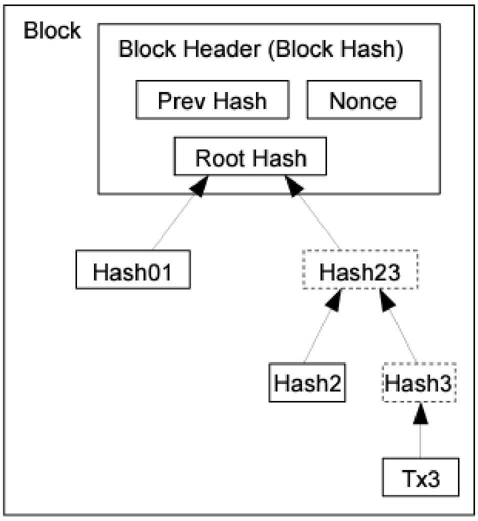
ప్రోత్సాహకం నోడ్‌లను నిజాయితీగా ఉంచడానికి ప్రేరేపించవచ్చు. ఒక లోభి దాడిదారుడు అన్ని నిజాయితీపరులైన నోడ్‌ల కంటే అధిక CPU శక్తిని సమకూర్చుకుంటే, అతను తన చెల్లింపులను వెనక్కి దోచుకోవడం ద్వారా ప్రజలను మోసగించడం లేదా కొత్త నాణేలను ఉత్పత్తి చేయడం అనే రెండింటిలో ఒకటి ఎంచుకోవాలి. అతను వ్యవస్థను మరియు తన స్వంత సంపద చెల్లుబాటును భంగపరచడం కంటే ఆట నియమాలను పాటించడం ద్వారా అందరినీ కలిపి కంటే అధిక కొత్త నాణేలను పొందే విధంగా అతనికి అనుకూలించే అటువంటి నియమాలను అధిక లాభదాయకంగా కనుగొనాలని భావించాలి.

7. డిస్క్ స్థలాన్ని పునఃప్రాప్తి

ఒక నాణెంలో చివరి లావాదేవీ చాలా బ్లాక్‌ల కింద పూర్తిగా సంగ్రహించబడిన తర్వాత, దాని కంటే ముందు ఖర్చు చేయబడిన లావాదేవీలను డిస్క్ స్థలం ఆదా చేయడానికి తొలగించవచ్చు. బ్లాక్‌ను యొక్క హాష్‌ను భంగపరచకుండా దీన్ని సులభతరం చేయడానికి, లావాదేవీలను ఒక మెర్కెల్ ట్రీ [7][2][5] లో హాష్ చేయబడుతాయి, దాని రూట్ మాత్రమే బ్లాక్‌ను యొక్క హాష్‌లో చేర్చబడుతుంది. పాత బ్లాక్‌లను ట్రీ యొక్క శాఖలను స్టబ్బింగ్ ఆఫ్ చేసి సంక్షిప్తం చేయవచ్చు. అంతర్గత హాష్‌లను నిల్వ చేయాల్సిన అవసరం లేదు.



Transactions Hashed in a Merkle Tree

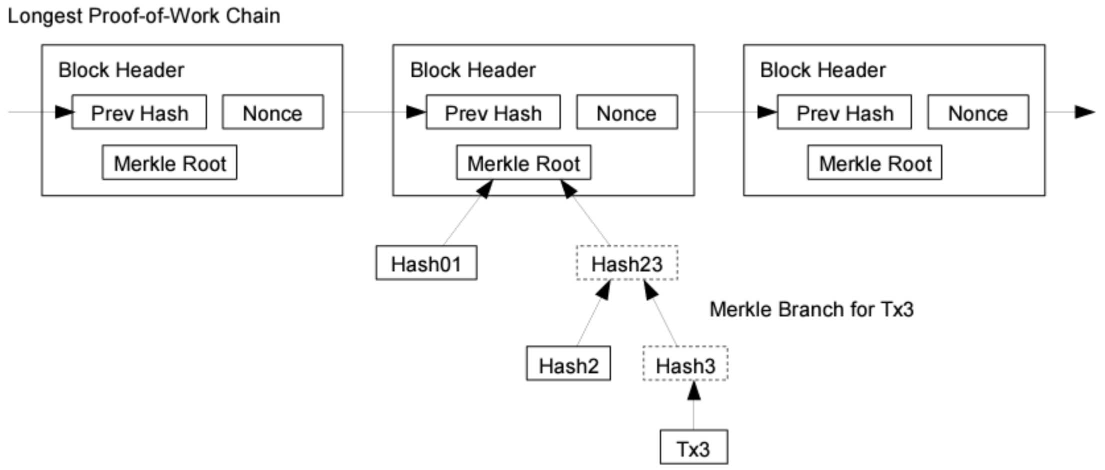


After Pruning Tx0-2 from the Block

లావాదేవీలు లేని ఒక బ్లాక్ హెడర్ సుమారు 80 బైట్లు ఉంటుంది. ప్రతి 10 నిమిషాలకు బ్లాక్‌లు ఉత్పత్తి అవుతాయని మనం ఊహిస్తే, 80 బైట్లు ★ 6 ★ 24 ★ 365 = సంవత్సరానికి 4.2MB. 2008 నాటికి కంప్యూటర్ సిస్టమ్‌లు సాధారణంగా 2GB ర్యామ్‌తో అమ్మబడుతుండగా, మూర్స్ సూత్రం 1.2GB ప్రతి సంవత్సరం వృద్ధిని ఊహించడం వల్ల, బ్లాక్ హెడర్‌లను మెమరీలో ఉంచాల్సిన పక్షంలో కూడా నిల్వ సమస్య ఉండకూడదు.

8. సరళీకృత చెల్లింపు తనిఖీ

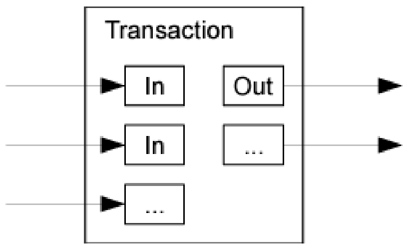
పూర్తి నెట్‌వర్క్ నోడ్‌ను నడపకుండానే చెల్లింపులను ధృవీకరించడం సాధ్యం. ఒక వినియోగదారుడు అతి పొడవైన ప్రూఫ్-ఆఫ్-వర్క్ చైన్ యొక్క బ్లాక్ హెడర్‌ల కాపీని మాత్రమే ఉంచుకోవాలి, దీనిని అతను అతి పొడవైన చైన్ తన వద్ద ఉందని నమ్మకం వచ్చేంత వరకు నెట్‌వర్క్ నోడ్‌లను ప్రశ్నించి పొందవచ్చు, మరియు లావాదేవీని దాని టైమ్‌స్టాంప్ చేయబడిన బ్లాక్‌కు లింక్ చేసే మెర్కెల్ శాఖను పొందవచ్చు. అతను లావాదేవీని తనకు తానుగా తనిఖీ చేయలేడు, కానీ దానిని చైన్‌లో ఒక స్థానంలో లింక్ చేసి, ఒక నెట్‌వర్క్ నోడ్ దానిని ఆమోదించిందని మరియు దాని తర్వాత జోడించబడిన బ్లాక్‌లు నెట్‌వర్క్ దానిని మరింత ధృవీకరించాయని చూడగలడు.



అలాగే, నెట్‌వర్క్‌ను నిజాయితీపరులైన నోడ్‌లు నియంత్రించే వరకు ధృవీకరణ విశ్వసనీయంగా ఉంటుంది, కానీ దాడిదారుడు నెట్‌వర్క్‌ను అధిగమించినప్పుడు అది మరింత అసురక్షితంగా మారుతుంది. నెట్‌వర్క్ నోడ్‌లు తమకు తాము లావాదేవీలను ధృవీకరించుకోగలరు, సరళీకృత పద్ధతిని దాడిదారుడు తయారు చేసిన లావాదేవీలతో దాడిదారుడు నెట్‌వర్క్‌ను అధిగమించగలిగినంత కాలం మోసగించవచ్చు. దీనిని నిరోధించే ఒక వ్యూహం అవాస్తవ బ్లాక్‌ను గుర్తించినప్పుడు నెట్‌వర్క్ నోడ్‌ల నుండి హెచ్చరికలను స్వీకరించడం, వినియోగదారు సాఫ్ట్‌వేర్‌ను పూర్తి బ్లాక్ మరియు హెచ్చరికలతో లావాదేవీలను డౌన్‌లోడ్ చేసి అసంగతిని నిర్ధారించడానికి ప్రేరేపించడం.తరచుగా చెల్లింపులు అందుకునే వ్యాపారాలు స్వతంత్ర భద్రత మరియు త్వరిత ధృవీకరణ కోసం తమ స్వంత నోడ్‌లను నడపడానికి బహుశా ఇంకా కోరుకుంటాయి.

9. విలువను కలపడం మరియు విడదీయడం

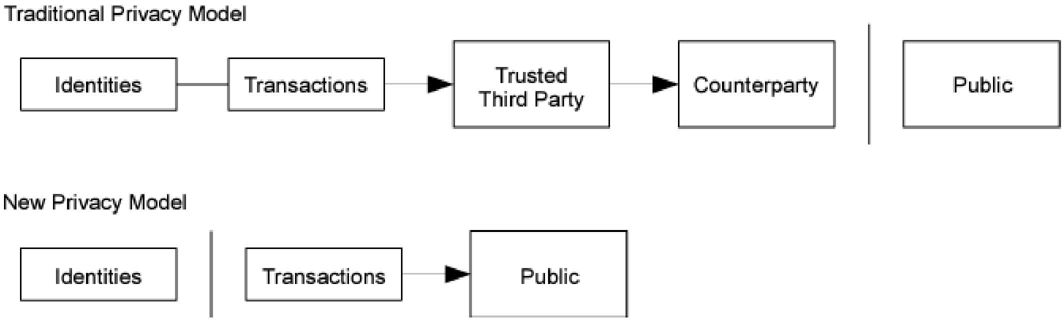
ప్రతి నాణెంను వ్యక్తిగతంగా నిర్వహించడం సాధ్యమైనప్పటికీ, బదిలీలో ప్రతి సెంట్ కోసం ఒక ప్రత్యేక లావాదేవీ చేయడం అసౌకర్యంగా ఉంటుంది. విలువను విభజించడానికి మరియు కలపడానికి, లావాదేవీలు బహుళ ఇన్‌పుట్‌లు మరియు ఔట్‌పుట్‌లను కలిగి ఉంటాయి. సాధారణంగా, గత లావాదేవీ నుండి ఒకే ఒక ఇన్‌పుట్ ఉంటుంది లేదా చిన్న మొత్తాలను కలిపే బహుళ ఇన్‌పుట్‌లు ఉంటాయి, మరియు గరిష్ఠంగా రెండు ఔట్‌పుట్‌లు ఉంటాయి: ఒకటి చెల్లింపు కోసం, మరొకటి మార్పు ఉంటే, దానిని పంపినవారికి తిరిగి ఇవ్వడానికి.



ఒక లావాదేవీ అనేక లావాదేవీల మీద ఆధారపడి ఉంటుంది, మరియు ఆ లావాదేవీలు మరిన్ని లావాదేవీల మీద ఆధారపడి ఉంటాయనే ఫ్యాన్-అవుట్ ఇక్కడ సమస్య కాదని గమనించాలి. ఒక లావాదేవీ చరిత్రను సంపూర్ణంగా స్వతంత్రంగా కాపీ చేయాల్సిన అవసరం ఎప్పుడూ ఉండదు.

10. గోప్యత

సాంప్రదాయిక బ్యాంకింగ్ మోడల్ సమాచారాన్ని పార్టీలకు మరియు విశ్వసనీయ మూడవ పార్టీకి మాత్రమే పరిమితం చేసి గోప్యతా స్థాయిని సాధిస్తుంది. అన్ని లావాదేవీలను బహిరంగంగా ప్రకటించాల్సిన అవసరం ఈ పద్ధతిని విడనాడేలా చేస్తుంది, కానీ మరొక చోట సమాచార ప్రవాహం తెగించడం ద్వారా గోప్యతను ఇంకా పాటించవచ్చు: పబ్లిక్ కీలను అజ్ఞాతంగా ఉంచుతూ. పబ్లిక్‌కు ఎవరో ఒకరు మరొకరికి ఒక మొత్తాన్ని పంపుతున్నారని తెలుసు, కానీ ఆ లావాదేవీని ఎవరికీ లింక్ చేయని సమాచారం లేకుండా. ఇది స్టాక్ ఎక్స్చేంజ్‌లు విడుదల చేసే సమాచార స్థాయికి సమానం, అక్కడ వ్యక్తిగత ట్రేడ్‌ల సమయం మరియు పరిమాణం, "టేప్", బహిరంగంగా చేయబడుతుంది, కానీ ఆ పార్టీలు ఎవరో చెప్పడం లేదు.



అదనపు ఫైర్‌వాల్‌గా, ప్రతి లావాదేవీకి కొత్త కీ జతను ఉపయోగించాలి, వాటిని సామాన్య యజమానితో లింక్ చేయకుండా ఉంచుటకు. బహుళ ఇన్‌పుట్ లావాదేవీలతో కొంత లింకింగ్ ఇంకా తప్పదు, ఇది తమ ఇన్‌పుట్‌లు ఒకే యజమాని యొక్కవి అని తప్పనిసరిగా బయటపెట్టుతుంది. రిస్క్ ఏమిటంటే, ఒక కీ యొక్క యజమాని గుర్తింపు బయటపడితే, లింకింగ్ అదే యజమాని చెందిన ఇతర లావాదేవీలను బయటపెట్టవచ్చు.

11. లెక్కింపులు

ఒక దాడిదారుడు నిజాయితీపరమైన చైన్ కంటే వేగంగా ఒక ప్రత్యామ్నాయ చైన్‌ను ఉత్పత్తి చేయాలని ప్రయత్నించే స్థితిని మనం పరిగణించుకుంటున్నాము. ఈ ప్రయత్నం సాధించబడినా, ఇది వ్యవస్థను స్వేచ్ఛాచారి మార్పులకు తెరువదు, ఉదాహరణకు ఖాళీ నుండి విలువను సృష్టించడం లేదా దాడిదారుడికి ఎప్పుడూ చెందని డబ్బును తీసుకోవడం. నోడ్‌లు చెల్లని లావాదేవీని చెల్లింపుగా అంగీకరించబోవు, మరియు నిజాయితీపరమైన నోడ్‌లు వాటిని కలిగి ఉన్న బ్లాక్‌ను ఎప్పుడూ అంగీకరించబోవు.

దాడిదారుడు తను ఇటీవల ఖర్చు చేసిన డబ్బును వెనక్కి తీసుకోవడానికి తన సొంత లావాదేవీని మార్చాలని ప్రయత్నించగలడు. నిజాయితీపరమైన చైన్ మరియు దాడిదారుడు చైన్ మధ్య జరిగే పోటీని బైనోమియల్ ర్యాండమ్ వాక్ గా వర్ణించవచ్చు. విజయ సంఘటన అనేది నిజాయితీపరమైన చైన్ ఒక బ్లాక్ ద్వారా విస్తరించబడి దాని ఆధిక్యతను +1 పెంచుకోవడం, మరియు వైఫల్య సంఘటన అనేది దాడిదారుడు చైన్ ఒక బ్లాక్ ద్వారా విస్తరించబడి అంతరాన్ని −1 తగ్గించడం.

ఒక నిర్దిష్ట లోటు నుండి దాడిదారుడు అందుకునే అవకాశం సూత్రప్రాయంగా జూదగాడు నాశనం సమస్యకు సమానం. పరిమితం లేని క్రెడిట్ తో ఒక జూదగాడు ఒక లోటుతో ప్రారంభించి సమతుల్యతను చేరడానికి అనంత సంఖ్యలో ప్రయత్నాలు చేయవచ్చు. అతను ఎప్పుడైనా సమతుల్యతను చేరుతాడా లేదా దాడిదారుడు నిజాయితీపరమైన చైన్‌ను అందుకుంటాడా అనే అవకాశాన్ని మనం ఈ విధంగా లెక్కించవచ్చు [8]:

p = *ఒక నిజాయితీ నోడ్ తదుపరి బ్లాక్ ని కనుగొనే సంభావ్యత*

q = *దాడి చేసేవాడు తదుపరి బ్లాక్ ని కనుగొనే సంభావ్యత*

q_z = *దాడి చేసేవాడు z బ్లాక్‌ల వెనకబడి ఉండి ఎప్పుడైనా సమానం చేయగలిగే సంభావ్యత*

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

మా ఊహానుసారం $p > q$ అయ్యేలాగా, దాడి చేసేవాడు సమానం చేయాల్సిన బ్లాక్‌ల సంఖ్య పెరిగే కొద్దీ సంభావ్యత వేగంగా తగ్గుతుంది. అతనికి వ్యతిరేకంగా పనులు ఉండగా, తొలి దశలో అదృష్టవంతమైన ప్రయత్నం చేయకపోతే, అతను మరింత వెనకబడుతూ ఉండగా అతని అవకాశాలు చాలా చిన్నవిగా మారిపోతాయి.

కొత్త లావాదేవీ పొందిన గ్రహీత సెండర్ లావాదేవీని మార్చలేరన్న నిర్ధారణకు సరిపడా కాలం ఎంత వేచి ఉండాలో మేము ఇప్పుడు పరిగణిస్తున్నాము. సెండర్ ఒక దాడి చేసేవాడుగా ఊహిస్తూ, అతను కొంతకాలం తనకు డబ్బులు చెల్లించాడని గ్రహీతను నమ్మించాలని కోరుకుంటాడు, తర్వాత కొంత సమయం గడిచాక దాన్ని తనకు తాను పే చేయడానికి మార్చుతాడు. అది జరిగినప్పుడు గ్రహీతకు హెచ్చరిక వస్తుంది, కానీ సెండర్ అది చాలా ఆలస్యమైపోయి ఉంటుందని ఆశిస్తాడు.

గ్రహీత కొత్త కీ జతను ఉత్పత్తి చేసి, సంతకం చేయబోయే కొద్ది సమయం ముందు పబ్లిక్ కీని సెండర్‌కు ఇస్తాడు. ఇది సెండర్‌ను అదృష్టం చాలా ముందుకు వెళ్లేంత వరకు నిరంతరం పని చేసి, ఆ క్షణంలో లావాదేవీని నిర్వహించే వరకు ముందుగా బ్లాక్‌ల చైన్‌ను తయారు చేసుకోలేకుండా చేస్తుంది. లావాదేవీ పంపిణీ అయ్యాక, అసత్యం చెప్పే సెండర్ తన లావాదేవీ యొక్క ప్రత్యామ్నాయ వెర్షన్‌ను కలిగి ఉన్న సమాంతర చైన్‌పై రహస్యంగా పని చేయడం ప్రారంభిస్తాడు.

గ్రహీత లావాదేవీ ఒక బ్లాక్‌లో చేర్చబడి, దాని తర్వాత z బ్లాక్‌లు అనుసంధానించబడే వరకు వేచి ఉంటాడు. అతనికి దాడి చేసేవాడు ఎంత పురోగతి సాధించాడు అనే ఖచ్చితమైన మొత్తం తెలియదు, కానీ నిజాయితీపరుడు ప్రతి బ్లాక్ కోసం సగటు అంచనా సమయం పటిష్టపడినట్లయితే, దాడి చేసేవాడి సాధ్యమైన పురోగతి ఒక పోయిస్సన్ వితరణతో ఉంటుంది మరియు అంచనా విలువ ఇలా ఉంటుంది:

$$\lambda = z\frac{q}{p}$$

దాడి చేసేవాడు ఇప్పుడు ఇంకా సమానం చేయగలిగే సంభావ్యతను పొందాలంటే, అతను సాధించి ఉండవచ్చు అన్ని పురోగతి మొత్తాల కోసం పోయిస్సన్ సాంద్రతను ఆ బిందువు నుండి అతను సమానం చేయగలిగే సంభావ్యతతో గుణిస్తాము:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \left\{ \begin{array}{cc} (q/p)^{(z-k)} & if\ k \le z \\ 1 & if\ k > z \end{array} \right\}$$

వితరణలోని అనంత తోకను కలపడం నివారించడానికి పునః విన్యాసం చేస్తూ...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

C కోడ్‌కు మార్చడం...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q /p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

కొన్ని ఫలితాలను నడుపుతూ, మనం చూడవచ్చు సంభావ్యత z తో వేగంగా తగ్గుతుందని.

```
q=0.1
z=0      P=1.000000
z=1      P=0.204583
z=2      P=0.050979
z=3      P=0.013172
z=4      P=0.003452
z=5      P=0.000917
z=6      P=0.0002428
z=7      P=0.0000647
z=8      P=0.0000173
z=9      P=0.0000046
z=10     P=0.0000012

q=0.3
z=0      P=1.0000000
```

```
z=5      P=0.1773523
z=10     P=0.0416605
z=15     P=0.0101008
z=20     P=0.0024804
z=25     P=0.0006132
z=30     P=0.0001522
z=35     P=0.0000379
z=40     P=0.0000095
z=45     P=0.0000024
z=50     P=0.0000006
```

P 0.1% కన్నా తక్కువగా ఉండేలా పరిష్కరించడం...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12. ముగింపు

మేము నమ్మకం ఆధారంగా లేకుండా ఎలక్ట్రానిక్ లావాదేవీల కోసం ఒక వ్యవస్థను సూచించాము. మేము డిజిటల్ సంతకాల నుండి తయారయ్యే నాణేల సాధారణ ఫ్రేమ్‌వర్క్‌తో ప్రారంభించాము, ఇది యజమానిత్వం యొక్క బలమైన నియంత్రణను అందిస్తుంది, కానీ డబుల్-స్పెండింగ్‌ను నివారించే మార్గం లేకుండా అసంపూర్ణం. ఈ సమస్యను పరిష్కరించడానికి, మేము ప్రూఫ్-ఆఫ్-వర్క్‌ను ఉపయోగించి లావాదేవీల యొక్క పబ్లిక్ చరిత్రను నమోదు చేసే పీర్-టు-పీర్ నెట్‌వర్క్‌ను సూచించాము, ఇది నిజాయితీ పూర్వక నోడ్‌లు సిపియు శక్తి యొక్క మెజారిటీని నియంత్రిస్తే దాడి చేసేవారికి మార్చడం గణనీయంగా అసాధ్యమైన వేగంగా మారుతుంది. నెట్‌వర్క్ దాని అమూర్త సాధారణత్వంలో గట్టిపడి ఉంది. నోడ్‌లు చాలా తక్కువ సమన్వయంతో అన్ని ఒకేసారి పని చేస్తాయి. వారు గుర్తించబడాల్సిన అవసరం లేదు, ఎందుకంటే సందేశాలు ఏ ప్రత్యేక ప్రదేశానికి నడపబడవు మరియు కేవలం ఉత్తమ ప్రయత్నం ఆధారంగా అందజేయాల్సిన అవసరం మాత్రమే ఉంది. నోడ్‌లు ఇష్టానుసారం నెట్‌వర్క్‌ను విడిచి మరియు చేరవచ్చు, వారు వెళ్లిపోయినప్పుడు ఏమి జరిగిందో గురించిన నిరూపణగా ప్రూఫ్-ఆఫ్-వర్క్ చైన్‌ను స్వీకరిస్తారు. వారు తమ సిపియు శక్తితో ఓటు వేస్తారు, చెల్లుబాటు అయ్యే బ్లాక్‌లను వాటిని పొడిగించడం ద్వారా మరియు చెల్లుబాటు కాని బ్లాక్‌లను పని చేయకుండా వాటిని తిరస్కరించడం ద్వారా తమ అంగీకారాన్ని వ్యక్తం చేస్తారు. ఏవైనా అవసరమైన నియమాలు మరియు ప్రేరణలను ఈ సమ్మతి యంత్రాంగంతో అమలు చేయవచ్చు.

మూలాలు

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.